ANNALES SCIENTIFIQUES DE L'É.N.S.

ALAN ADOLPHSON
STEVEN SPERBER

p-adic estimates for exponential sums and the theorem of Chevalley-Warning

Annales scientifiques de l'É.N.S. 4e série, tome 20, nº 4 (1987), p. 545-556
<http://www.numdam.org/item?id=ASENS_1987_4_20_4_545_0>

Ann. scient. Éc. Norm. Sup.,
4[e] série, t. 20, 1987, p. 545 à 556.

p-ADIC ESTIMATES FOR EXPONENTIAL SUMS AND THE THEOREM OF CHEVALLEY-WARNING

BY ALAN ADOLPHSON (1) AND STEVEN SPERBER (2)

1. Introduction

The purpose of this article is to give an estimate for the p-divisibility of a general exponential sum over a finite field k of characteristic p. Since exponential sums can be used, in a well-known manner, to count the number of rational points on a variety in characteristic p, we obtain as a corollary an estimate for the p-divisibility of the number of rational points. This estimate improves the classical theorem of Chevalley-Warning [17], which states that the number of common zeros in k of polynomials $g_1, \ldots, g_m$ of degrees $d_1, \ldots, d_m$ in n variables with $\sum_{i=1}^{m} d_i < n$ is divisible by p. Our work also improves recent work of Sperber [16] on exponential sums, and the application to counting points on a variety improves recent generalizations of the Chevalley-Warning Theorem due to Ax [4] and Katz [10].

These earlier results have the common feature of estimating the p-divisibility in terms of the number of variables and degrees of the polynomials involved. Let k be the finite field with $q=p^a$ elements, let $g_1, \ldots, g_m$ be polynomials over k of degrees $d_1, \ldots, d_m$, respectively, and let V be the variety defined by the common vanishing of the g_i. Let μ be the least nonnegative integer $\geqq \mu_0$, where

$$\mu_0 = \frac{n - \sum_{i=1}^{m} d_i}{\max\{d_i\}}.$$

The theorem of Katz asserts that the number of k-rational points on V is divisible by q^{μ}. This implies the earlier results of Ax and Chevalley-Warning.

(1) Partially supported by N.S.F. Grant No. DMS-8601872.
(2) Partially supported by N.S.F. Grant No. DMS-8601461.

Our work gives a qualitative improvement by taking into account which monomials actually occur in the given polynomials. Let Ψ be a nontrivial additive character of k. For any polynomial $f \in k[x_1, \ldots, x_n]$ we form the exponential sum

$$(1.1) \qquad S(f) = \sum_{x_1, \ldots, x_n \in k} \Psi(f(x_1, \ldots, x_n)) \in \mathbf{Q}(\zeta_p),$$

where ζ_p is a primitive p-th root of unity. We shall assume that f is not a polynomial in some proper subset of the variables $x_1, \ldots, x_n$. This involves no loss of generality, for if $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_a)$ with $a < n$, then $S(f) = q^{n-a} S(g)$; so a p-adic estimate for $S(f)$ is a trivial consequence of a p-adic estimate for $S(g)$.

Let $\Delta(f)$ be the Newton polyhedron of f (the definition of Newton polyhedron is recalled in section 2). Let $\omega(f)$ be the smallest positive rational number such that $\omega(f)\Delta(f)$, the dilation of $\Delta(f)$ by the factor $\omega(f)$, contains a lattice point with all coordinates positive. Let ord_q be an additive valuation on $\mathbf{Q}(\zeta_p)$, lying over p and normalized by the condition $\operatorname{ord}_q q = 1$. Our main result is:

THEOREM 1.2. — *If f is not a polynomial in some proper subset of the variables $x_1, \ldots, x_n$, then*

$$\operatorname{ord}_q S(f) \geqq \omega(f).$$

If f has degree d, then $\omega(f) \geqq n/d$ (*see* section 5). Hence:

COROLLARY 1.3. — *Under the hypotheses of Theorem* 1.2, $\operatorname{ord}_q S(f) \geqq n/d$.

Theorem 1.2 will be shown to imply the theorems of Katz and Sperber.

Katz used his result to extract a lower bound for the slope of the first side of the Newton polygon of the primitive middle-dimensional factor of the zeta function of a smooth projective complete intersection. Deligne [6], using Hirzebruch's formula for the Hodge numbers of a complete intersection, had calculated the first nonvanishing primitive Hodge number, and Katz's result shows that the first slope of the Newton polygon is at least as large as the first slope of the Hodge polygon (*see* [10], Conjecture 2.9 for the definition of the Hodge polygon). Dwork [8], section 7, had already shown that the Newton polygon of the primitive middle-dimensional factor of the zeta function of a smooth projective hypersurface lies over its Hodge polygon, so Katz was led to conjecture that this relationship holds for smooth projective complete intersections as well. This conjecture was subsequently proved by Mazur [13].

By [4], section 1, our result may be interpreted as giving a lower bound for the first slope of the Newton polygon of the **L**-function associated to the exponential sum. In a future article we shall determine, under certain restrictions on the exponential sum (namely, that it be nondegenerate and commode in the sense of [11], which forces the **L**-function to be a polynomial), a lower bound for the entire Newton polygon of this **L**-function. We believe that this lower bound is also connected with Hodge theory.

Consider the equation $f(x_1, \ldots, x_n) = N$, where $f \in \mathbf{Z}[x_1, \ldots, x_n]$ has positive integer coefficients and N is a positive integer. Our work implies that when $\omega(f) > 1$, the congruence $f(x_1, \ldots, x_n) \equiv N \pmod{p}$ for any prime p has at least $p^{\omega(f)-1}$ solutions, provided that it has at least one solution. We believe these congruences have so many solutions because the equation $f(x_1, \ldots, x_n)=\mathrm{N}$ has many solutions in positive integers. More precisely, we conjecture that if $\omega(f)>1$ and if there are no congruence obstructions, the number of solutions in positive integers of $f(x_1, \ldots, x_n)=\mathrm{N}$ grows like $\mathrm{N}^{\omega(f)-1}$. We shall return to this question in a future article.

The outline of the paper is as follows. In section 2 we derive two consequences of Theorem 1.2 (Theorems 2.11 and 2.14) which generalize the theorems of Katz and Sperber, respectively. We also give some examples to show that our work gives a strict improvement over previous results. Sections 3 and 4 are devoted to the proof of Theorem 1.2. In section 5 we show how Corollary 1.3 and the theorems of Katz and Sperber follow from taking the largest possible Newton polyhedron that can occur in Theorems 1.2, 2.11, and 2.14, respectively. Finally, in section 6, we discuss some connections with other recent work.

We would like to thank Pierrette Cassou-Nogues for some very helpful discussions.

2. Statement of further results

Let $\mathbf{N}$ denote the nonnegative integers and write $j=(j_1, \ldots, j_n)\in\mathbf{N}^n$, $x=(x_1, \ldots, x_n)$, $x^j=x_1^{j_1}\ldots x_n^{j_n}$. For $f\in k[x_1, \ldots, x_n]$, write

$$f=\sum_{j\in\mathrm{J}} a_j x^j, \tag{2.1}$$

where J is a finite subset of $\mathbf{N}^n$. Let $\mathscr{A}$ be the $(n\times|\mathrm{J}|)$-matrix whose columns are the $j=(j_1, \ldots, j_n)\in\mathrm{J}$. Given $r\in\mathbf{N}^n$, consider the matrix equation

$$\mathscr{A}\begin{pmatrix} u_1 \\ \vdots \\ u_{|\mathrm{J}|}\end{pmatrix}=\begin{pmatrix} r_1 \\ \vdots \\ r_n\end{pmatrix}. \tag{2.2}$$

We define a weight function w_f by

$$w_f(r)=\inf\{u_1+\ldots+u_{|\mathrm{J}|}\}, \tag{2.3}$$

where the inf is taken over all nonnegative rational solutions $u=(u_1, \ldots, u_{|\mathrm{J}|})$ of (2.2) and we put $w_f(r)=+\infty$ if there are no such solutions.

This inf can be calculated by standard techniques in linear programming, which also show that the infimum is in fact a minimum, but it seems more useful to have a geometric description of w_f. The Newton polyhedron $\Delta(f)$ is defined to be the convex hull in $\mathbf{R}^n$ of the set $\mathrm{J}\cup\{(0, \ldots, 0)\}$. Let $\mathbf{R}_+\langle f\rangle$ denote the subset of $\mathbf{R}^n$ consisting of all linear combinations with nonnegative real coefficients of elements of J. Then $\mathbf{R}_+\langle f\rangle$ is the union of all rays emanating from the origin and passing through $\Delta(f)$. Equation (2.2) has a solution u whose components are nonnegative rational numbers if and only if $r\in\mathbf{R}_+\langle f\rangle$. Thus $w_f(r)=+\infty$ if and only if $r\notin\mathbf{R}_+\langle f\rangle$. If $r\in\mathbf{R}_+\langle f\rangle$, the ray emanating from the origin and passing through r intersects $\Delta(f)$ in a face that does not contain the origin. Let $\sum_{i=1}^{n}\alpha_i\mathrm{X}_i=1$ be the equation of a hyperplane passing through this face (this hyperplane is not uniquely determined unless the face has dimension $n-1$). Then by standard arguments in linear programming,

$$(2.4)\qquad w_f(r)=\sum_{i=1}^{n}\alpha_i r_i.$$

We have immediately [3], Lemma 2.14:

LEMMA 2.5. — *(a) If k is a nonnegative integer, then $w_f(kr)=kw_f(r)$.*

(b) If $w_f(r)$, $w_f(r')<+\infty$, then $w_f(r+r')<+\infty$. Furthermore,

$$w_f(r+r')\leqq w_f(r)+w_f(r').$$

(c) There exists a positive integer M such that $w_f(\mathbf{N}^n)\subseteq(1/\mathrm{M})\mathbf{N}\cup\{+\infty\}$.

Let $\mathbf{N}_+$ denote the positive integers and set

$$(2.6)\qquad \omega(f)=\min_{r\in(\mathbf{N}_+)^n}\{w_f(r)\}.$$

Equivalently, $\omega(f)$ is the smallest positive rational number such that $\omega(f)\Delta(f)$ contains a point of $(\mathbf{N}_+)^n$.

Let V be the variety over k defined by the common vanishing of polynomials $g_1, \ldots, g_m\in k[x_1, \ldots, x_n]$ and let N(V) be the number of k-rational points on V. Then

$$(2.7)\qquad q^m\,\mathrm{N}(\mathrm{V})=\sum_{\substack{x_1, \ldots, x_n\in k\\ y_1, \ldots, y_m\in k}}\Psi\left(\sum_{i=1}^{m}y_i g_i(x_1, \ldots, x_n)\right)(=\mathrm{S}(\textstyle\sum y_i g_i)).$$

Suppose $g_1, \ldots, g_m$ are not all polynomials in some proper subset of $x_1, \ldots, x_n$. Then from Theorem 1.2 we get

$$(2.8)\qquad \mathrm{ord}_q\,\mathrm{N}(\mathrm{V})\geqq\omega(\textstyle\sum y_i g_i)-m.$$

When V is a hypersurface, this estimate has a simple consequence:

COROLLARY 2.9. — *Let V be the hypersurface defined by the equation $g(x_1, \ldots, x_n)=0$. If $\Delta(yg)$ does not contain a point of $(\mathbf{N}_+)^{n+1}$, then N(V) is divisible by q.*

To see that this is a strict improvement over Chevalley-Warning, suppose that g has degree n, i. e., the number of variables equals the degree. Then Chevalley-Warning gives no information, but the hypothesis of the corollary will be satisfied when the point $(1, \ldots, 1)$ does not lie in the convex hull of the set of exponents of monomials of degree n occuring in g. For example, if the only monomial of degree n occuring in g is x^j and if $x^j\neq x_1\ldots x_n$, then this condition is satisfied so N(V) is divisible by q.

We can say more about $\omega(\sum y_i g_i)$. If we let $y_1, \ldots, y_m$ correspond to the last m rows of $\mathscr{A}$ and write the right-hand side of (2.2) as $(r_1, \ldots, r_n; s_1, \ldots, s_m)^t$, then

$$u_1+\ldots+u_{|\mathrm{J}|}=s_1+\ldots+s_m.$$

Thus

$$(2.10)\qquad \omega(\sum y_i g_i)=\min\left\{\sum_{i=1}^{m} s_i \,\middle|\, (r;\, s)\in \mathbf{R}_+ \langle \sum y_i g_i \rangle \cap (\mathbf{N}_+)^{n+m}\right\}.$$

Equation (2.8) implies immediately:

THEOREM 2.11. — *If $g_1, \ldots, g_m$ are not all polynomials in some proper subset of $x_1, \ldots, x_n$, then*

$$(2.12)\qquad \operatorname{ord}_q \mathrm{N}(\mathrm{V}) \geqq \min\left\{\sum_{i=1}^{m} s_i \,\middle|\, (r;\, s)\in \mathbf{R}_+ \langle \sum y_i g_i \rangle \cap (\mathbf{N}_+)^{n+m}\right\}-m.$$

For example, suppose V is the hypersurface

$$a_1 x_1^{j_1}+\ldots+a_n x_n^{j_n}=0.$$

Set $d_i=(j_i,\, q-1)$. For $\alpha_i \in \{1/d_i, \ldots, (d_i-1)/d_i\}$, let χ_{α_i} be the multiplicative character on $k^\times$ defined by sending a generator to $e^{2\pi\sqrt{-1}\alpha_i}$. For each n-tuple $\alpha=(\alpha_1, \ldots, \alpha_n)$, define a Jacobi sum $\mathrm{J}(\alpha)$ by

$$\mathrm{J}(\alpha)=\sum_{u_1+\ldots u_n=0} \prod_{i=1}^{n} \chi_{\alpha_i}(u_i).$$

According to Weil's calculation [18],

$$\mathrm{N}(\mathrm{V})=q^{n-1}+\frac{1}{q-1}\sum_{\alpha_1+\ldots+\alpha_n\in \mathbf{Z}} \mathrm{J}(\alpha).$$

If the j_i are relatively prime, then so are the d_i and there are no n-tuples α satisfying $\alpha_1+\ldots+\alpha_n \in \mathbf{Z}$. Hence $\mathrm{N}(\mathrm{V})=q^{n-1}$ and $\operatorname{ord}_q \mathrm{N}(\mathrm{V})=n-1$. In general, Katz's theorem does not predict any divisibility by p in this case. However, an easy calculation shows that the right-hand side of (2.12) equals $n-1$, hence Theorem 2.11 is sharp in this example.

Finally, we note that we can generalize further to the case of an exponential sum on the variety V. Take $f\in k[x_1, \ldots, x_n]$ and let $\mathrm{V}(k)$ be the set of k-rational points of V. Define

$$\mathrm{S}(\mathrm{V}, f)=\sum_{(x_1, \ldots, x_n)\in \mathrm{V}(k)} \Psi(f(x_1, \ldots, x_n)).$$

Then $\mathrm{S}(\mathrm{V}, f)=q^{-m}\mathrm{S}(f+\sum y_i g_i)$ and an argument similar to the derivation of (2.10) shows that

$$(2.13)\quad \omega(f+\sum y_i g_i)=\min\left\{t+\sum_{i=1}^{m} s_i \,\middle|\, (r;\, s;\, t)\in \mathbf{R}_+ \langle zf+\sum y_i g_i \rangle \cap ((\mathbf{N}_+)^{n+m}\times \mathbf{Q}_+)\right\},$$

where $\mathbf{Q}_+$ denotes the nonnegative rationals. Thus Theorem 1.2 implies:

THEOREM 2.14. — *If f, $g_1, \ldots, g_m$ are not all polynomials in some proper subset of $x_1, \ldots, x_n$, then*

$$\operatorname{ord}_q S(V, f) \geqq \min\left\{ t + \sum_{i=1}^{m} s_i \,\middle|\, (r; s; t) \in \mathbf{R}_+ \langle zf + \sum y_i g_i \rangle \cap ((\mathbf{N}_+)^{n+m} \times \mathbf{Q}_+) \right\} - m.$$

3. Trace formula

To prove Theorem 1.2 it is convenient to consider also the exponential sums $S^*(f)$ defined by

$$S^*(f) = \sum_{x_1, \ldots, x_n \in k^\times} \Psi(f(x_1, \ldots, x_n)). \tag{3.1}$$

They are related to our basic exponential sums $S(f)$ in the following way. Put $S = \{1, 2, \ldots, n\}$. For any subset $A \subseteq S$, let f_A be the polynomial obtained from f by setting $x_i = 0$ for $i \in A$. Let $|A|$ denote the cardinality of A. Then

$$S(f) = \sum_{A} S^*(f_A) \tag{3.2}$$

$$S^*(f) = \sum_{A} (-1)^{|A|} S(f_A). \tag{3.3}$$

We recall some basic facts about the sums $S^*(f_A)$ from our earlier article [3]. These facts were proved there for the case $A = S$, but the arguments in the general case are identical. Let Ω be the completion of an algebraic closure of the p-adic numbers $\mathbf{Q}_p$ and let "ord" denote the additive valuation on Ω normalized by $\operatorname{ord} p = 1$. Let $E(t)$ be the Artin-Hasse exponential series:

$$E(t) = \exp\left(\sum_{m=0}^{\infty} \frac{t^{p^m}}{p^m} \right) \in (\mathbf{Z}_p \cap \mathbf{Q})[[t]]. \tag{3.4}$$

Let $\gamma \in \Omega$ be a root of $\sum_{m=0}^{\infty} t^{p^m}/p^m = 0$ satisfying $\operatorname{ord} \gamma = 1/(p-1)$. The series

$$\theta(t) = E(\gamma t) = \sum_{m=0}^{\infty} \lambda_m t^m \tag{3.5}$$

is a splitting function in Dwork's terminology [7], section 4 and its coefficients satisfy

$$\operatorname{ord} \lambda_m \geqq \frac{m}{p-1}, \qquad \lambda_m \in \mathbf{Q}_p(\gamma). \tag{3.6}$$

Furthermore, one has $\mathbf{Q}_p(\gamma) = \mathbf{Q}_p(\zeta_p)$.

Let K denote the unramified extension of $\mathbf{Q}_p$ in Ω of degree a, where $q=p^a$. For f as in (2.1), let

$$\hat{f}=\sum_{j \in \mathrm{J}} \hat{a}_j x^j \in \mathrm{K}[x_1, \ldots, x_n] \tag{3.7}$$

be its Teichmüller lifting, i.e., $(\hat{a}_j)^q=\hat{a}_j$. Let τ be the Frobenius automorphism of K, which is extended to $\mathrm{K}(\zeta_p)$ by defining $\tau(\zeta_p)=\zeta_p$. Set

$$\mathrm{F}(x)=\prod_{j \in \mathrm{J}} \theta(\hat{a}_j x^j) \in \mathrm{K}(\zeta_p)[[x]] \tag{3.8}$$

$$\mathrm{F}_0(x)=\prod_{i=0}^{a-1} {}^{\tau_i}\mathrm{F}(x^{p^i}) \in \mathrm{K}(\zeta_p)[[x]] \tag{3.9}$$

We denote by F_{A} and $\mathrm{F}_{0,\mathrm{A}}$ the corresponding series in $\mathrm{K}(\zeta_p)[[\{x_i\}_{i \in \mathrm{S} \setminus \mathrm{A}}]]$ obtained by starting with f_{A} in place of f.

Let $\mathrm{L}(b)$ be the space of all power series $\sum_{r \in \mathbf{Z}^n} \mathrm{A}_r x^r \in \Omega[[x]]$ satisfying

$$\operatorname{ord} \mathrm{A}_r \geqq b w_f(r)+O(1). \tag{3.10}$$

In particular, this means $\mathrm{A}_r=0$ if $w_f(r)=+\infty$. By [3], section 2,

$$\mathrm{F} \in \mathrm{L}\left(\frac{1}{p-1}\right), \qquad \mathrm{F}_0 \in \mathrm{L}\left(\frac{p}{q(p-1)}\right). \tag{3.11}$$

Define an operator ψ on power series by

$$\psi\left(\sum \mathrm{A}_r x^r\right)=\sum \mathrm{A}_{pr} x^r.$$

Let $\iota: \mathrm{L}(p/(p-1)) \hookrightarrow \mathrm{L}(p/q(p-1))$ be the canonical injection and denote by α the composition

$$\mathrm{L}\left(\frac{p}{p-1}\right) \overset{\iota}{\hookrightarrow} \mathrm{L}\left(\frac{p}{q(p-1)}\right) \xrightarrow{\mathrm{F}_0} \mathrm{L}\left(\frac{p}{q(p-1)}\right) \xrightarrow{\psi^a} \mathrm{L}\left(\frac{p}{p-1}\right),$$

where the middle arrows means "multiplication by F_0". It follows from Serre [15] that the trace $\operatorname{Tr}(\alpha \mid \mathrm{L}(p/(p-1)))$ is well-defined. The Dwork trace formula asserts that

$$\mathrm{S}^*(f)=(q-1)^n \operatorname{Tr}\left(\alpha \,\middle|\, \mathrm{L}\left(\frac{p}{p-1}\right)\right), \tag{3.12}$$

where the nontrivial additive character implicit on the left-hand side is derived from the splitting function $\theta(t)$.

A similar formula is valid for $\mathrm{S}^*(f_{\mathrm{A}})$. Denote by $\mathrm{L}_{(\mathrm{A})}(b)$ the space of power series $\sum \mathrm{A}_r x^r \in \Omega[[\{x_i\}_{i \in \mathrm{S} \setminus \mathrm{A}}]]$ satisfying the growth condition (3.10) (note that $w_f|_{\mathbf{R}^{n-|\mathrm{A}|}}=w_{f_{\mathrm{A}}}$), and denote by α_{A} the endomorphism of $\mathrm{L}_{(\mathrm{A})}(p/(p-1))$ defined in analogy with α using $\mathrm{F}_{0,\mathrm{A}}$ in place of F_0. Then one has

$$\mathrm{S}^*(f_{\mathrm{A}})=(q-1)^{n-|\mathrm{A}|} \operatorname{Tr}\left(\alpha_{\mathrm{A}} \,\middle|\, \mathrm{L}_{(\mathrm{A})}\left(\frac{p}{p-1}\right)\right). \tag{3.13}$$

By repeating the argument of [14], Lemma 7.4 (2), one can derive from (3.13) a trace formula for $S(f)$ itself. Set

$$L_A\left(\frac{p}{p-1}\right)=\left\{\sum_{j\in\mathbf{N}^n} A_j x^j \in L\left(\frac{p}{p-1}\right)\middle| j_i>0 \text{ for all } i\in A\right\}.$$

Note that $L_A(p/(p-1))$ is stable under α and that $\operatorname{Tr}(\alpha\,|\,L_A(p/(p-1)))$ is well-defined. Then

$$S(f)=\sum_{A\subseteq S}(-1)^{|A|}q^{n-|A|}\operatorname{Tr}(\alpha\,|\,L_A(p/(p-1))). \tag{3.14}$$

4. Proof of Theorem 1.2

For convenience we denote $L_A(p/(p-1))$ by L_A. From equation (3.14) it follows that

$$\operatorname{ord}_q S(f)\geqq\min_{A\subseteq S}\{n-|A|+\operatorname{ord}_q\operatorname{Tr}(\alpha\,|\,L_A)\}. \tag{4.1}$$

We first estimate $\operatorname{ord}_q\operatorname{Tr}(\alpha\,|\,L_A)$.

By Lemma 2.5 (*c*), we may define for each $A\subseteq S$ a function $W_A: N\to N$ by

$$W_A(k)=\operatorname{card}\left\{r\in\mathbf{N}^n\,\middle|\,w_f(r)=\frac{k}{M}\text{ and } r_i>0 \text{ for all } i\in A\right\}.$$

The series

$$\det(I-t\alpha\,|\,L_A)\overset{\text{def}}{=}\exp\left(-\sum_{m=0}^{\infty}\operatorname{Tr}(\alpha^m\,|\,L_A)\frac{t^m}{m}\right)$$

is a p-adic entire function, i. e., it converges for all $t\in\Omega$ ([15], see also [3], section 2).

PROPOSITION 4.2. — *For* $A\subseteq S$, *the Newton polygon of* $\det(I-t\alpha\,|\,L_A)$ *computed with respect to* ord_q *lies above the polygon with vertices* (0, 0) *and*

$$\left(\sum_{k=0}^{l}W_A(k),\ \frac{1}{M}\sum_{k=0}^{l}k\,W_A(k)\right),\qquad l=0,1,2,\ldots$$

Proof. — The case $A=\varnothing$ is the content of [3], Proposition 3.13. The general case is proved by an identical argument. □

Set

$$\omega_A(f)=\min\{w_f(r)\,|\,r\in\mathbf{N}^n \text{ and } r_i>0 \text{ for all } i\in A\}.$$

Since $-\operatorname{Tr}(\alpha\,|\,L_A)$ is the coefficient of t in $\det(I-t\alpha\,|\,L_A)$ we have immediately:

COROLLARY 4.3. — $\operatorname{ord}_q\operatorname{Tr}(\alpha\,|\,L_A)\geqq\omega_A(f)$.

From (4.1) we then have

$$\operatorname{ord}_q S(f)\geqq\min_{A\subseteq S}\{n-|A|+\omega_A(f)\}. \tag{4.4}$$

Since $\omega_S(f)=\omega(f)$, Theorem 1.2 will be established if we can show that the minimum on the right-hand side of (4.4) occurs for $A=S$. But this is an immediate consequence of:

LEMMA 4.5. — *Suppose* $A \subseteqq S$ *and* $\beta \in S \setminus A$. *Then*

$$\omega_{A \cup \{\beta\}}(f) \leqq \omega_A(f)+1.$$

Proof. — From the definitions of $\omega_A(f)$ and w_f, there exists a $|J|$-tuple $u=(u_1, \ldots, u_{|J|})$ of nonnegative rational numbers and an n-tuple $r=(r_1, \ldots, r_n)$ of nonnegative integers with $r_i>0$ for $i \in A$ such that $\mathscr{A} u=r$ and

$$\omega_A(f)=u_1+\ldots+u_{|J|}.$$

If $r_\beta \neq 0$, then from the definition of $\omega_{A \cup \{\beta\}}(f)$ we have $\omega_{A \cup \{\beta\}}(f)=\omega_A(f)$. Suppose $r_\beta=0$. Not all entries in the β-th row of $\mathscr{A}$ can vanish, since we assumed f could not be written as a polynomial in some proper subset of the variables $x_1, \ldots, x_n$. Suppose the entry in column ν, row β is >0. Since $r_\beta=0$ we must have $u_\nu=0$. Let u' be the $|J|$-tuple obtained from u by putting 1 in the ν-th entry and leaving the other entries unchanged. Define $r'=(r'_1, \ldots, r'_n)$ by $r'=\mathscr{A} u'$. Then $r'_i \geqq r_i$ for $i=1, \ldots, n$, and $r'_\beta>0$, so

$$\omega_{A \cup \{\beta\}}(f) \leqq \sum_{i=1}^{|J|} u'_i=\omega_A(f)+1. \ \square$$

5. Theorems of Katz and Sperber

For any convex polyhedron Δ in $\mathbf{R}^n$ with one vertex at the origin, let $\omega(\Delta)$ be the smallest positive rational number such that $\omega(\Delta)\Delta$ contains a point of $(\mathbf{N}_+)^n$. If $\Delta(f) \subseteqq \Delta$, then we have clearly $\omega(f) \geqq \omega(\Delta)$, so by Theorem 1.2

$$(5.1) \qquad \operatorname{ord}_q S(f) \geqq \omega(\Delta).$$

For example, if f has degree d, then $\Delta(f)$ is contained in the simplex Δ whose vertices are the origin and the points $d\mathbf{e}_1, \ldots, d\mathbf{e}_n$, where $\mathbf{e}_j$ is the point with 1 in the j-th coordinate and zeros elsewhere. Clearly, $(1, \ldots, 1) \in (n/d)\Delta$ but $(\kappa\Delta) \cap (\mathbf{N}_+)^n=\varnothing$ if $\kappa<n/d$, hence $\omega(\Delta)=n/d$. Thus (5.1) implies Corollary 1.3.

The theorem of Katz can be derived in similar fashion. In the notation of Theorem 2.11, if g_i has degree d_i and $\mathbf{e}_j$, $j=1, \ldots, n$ (resp. $\mathbf{e}'_i$, $i=1, \ldots, m$) denotes the point in $\mathbf{R}^{n+m}$ with coordinate 1 in the j-th entry [resp. the $(n+i)$-th entry] and zeros elsewhere, then $\Delta(\sum y_i g_i) \subseteqq \mathbf{R}^{n+m}$ lies in the polyhedron Δ with vertices at the origin, $\mathbf{e}'_i$ $(i=1, \ldots, m)$, and $d_i\mathbf{e}_j+\mathbf{e}'_i$ $(j=1, \ldots, n;\ i=1, \ldots, m)$. In fact, Δ is the largest polyhedron that can occur as the Newton polyhedron of some $\sum y_i g_i$, given the number of variables and the degrees of the g_i. We have from (2.8)

$$(5.2) \qquad \operatorname{ord}_q N(V) \geqq \omega(\Delta)-m.$$

Let μ be the least nonnegative integer $\geqq \mu_0$, where

$$\mu_0 = \frac{n - \sum_{i=1}^{m} d_i}{\max\{d_i\}}.$$

We shall show that

$$(5.3) \qquad \omega(\Delta) = \mu + m,$$

hence (5.2) implies the theorem of Katz.

The polyhedron Δ is bounded by the hyperplanes $x_j = 0$, $y_i = 0$, and the two hyperplanes $y_1 + \ldots + y_m = 1$ (which contains all vertices except the origin) and

$$(5.4) \qquad x_1 + \ldots + x_n = d_1 y_1 + \ldots + d_m y_m$$

(which contains all vertices except the $\mathbf{e}'_i$). Let $\mathbf{R}_+ \langle \Delta \rangle$ be the cone defined by the inequalities $x_j \geqq 0$, $y_i \geqq 0$, and

$$(5.5) \qquad x_1 + \ldots + x_n \leqq d_1 y_1 + \ldots + d_m y_m.$$

The same argument that proved (2.10) shows that

$$(5.6) \qquad \omega(\Delta) = \min\left\{ \sum_{i=1}^{m} s_i \,\middle|\, (r; s) \in \mathbf{R}_+ \langle \Delta \rangle \cap (\mathbf{N}_+)^{n+m} \right\}.$$

Suppose for convenience that $d_m = \max\{d_i\}$. Inequality (5.5) is equivalent to

$$(5.7) \qquad \frac{\sum_{j=1}^{n} x_j + \sum_{i=1}^{m} (d_m - d_i) y_i}{d_m} \leqq y_1 + \ldots + y_m.$$

The min of the left-hand side of (5.7) on $(\mathbf{N}_+)^{n+m}$ occurs when all x_j and y_i equal 1, hence by (5.6), $\omega(\Delta) \geqq \mu + m$. But the point $x_j = 1$ for $j = 1, \ldots, n$, $y_i = 1$ for $i = 1, \ldots, m-1$, $y_m = \mu + 1$ satisfies (5.7) [hence satisfies (5.5)], therefore lies in $\mathbf{R}_+ \langle \Delta \rangle \cap (\mathbf{N}_+)^{n+m}$. It then follows from (5.6) that $\omega(\Delta) \leqq \mu + m$ also, so (5.3) is established.

Assume the notation and hypotheses of Theorem 2.14, and let degree $f = d_0$. Sperber's theorem is the assertion that $\mathrm{ord}_q \mathrm{S}(\mathrm{V}, f) \geqq \mu'$, where μ' is the least element of $d_0^{-1}\mathbf{N}$ that is $\geqq \mu'_0$, where

$$\mu'_0 = \frac{n - \sum_{i=1}^{m} d_i}{\max\{d_i\}_{i=0}^{m}}.$$

It can be derived similarly, by considering the largest possible Newton polyhedron that can occur in Theorem 2.14 when the degrees of the given polynomials are specified.

6. Connections with recent work

LEMMA **6.1.** — *Suppose every face of* $\Delta(f)$ *of codimension* 1 *that does not contain the origin lies in a hyperplane* $\sum_{i=1}^{n} \alpha_i X_i = 1$ (*a so-called hyperplane of support*) *where all* $\alpha_i \geqq 0$. *Suppose also that* $(1, \ldots, 1) \in \mathbf{R}_+ \langle f \rangle$. *Then* $\omega(f) = \omega_f(1, \ldots, 1)$.

Proof. — Set $P_0 = (1, \ldots, 1)$, $O = (0, \ldots, 0)$. Let Γ be the hyperplane of support intersecting the ray $O P_0$, say, in the point Q. Let Γ_0 be the hyperplane passing through P_0 parallel to Γ. If P is any other point in $\mathbf{Z}^n$ with all coordinates positive then Γ_0 separates O and P. Let the ray O P intersect the hyperplane Γ_0 in R_0 (so $|O R_0| \leqq |O P|$). Suppose proceeding along the ray O P from O that the first hyperplane of support that O P intersects is $\tilde{\Gamma}$, say, in the point $\tilde{R}$. Suppose it intersects Γ in the point R. Then the convexity of $\Delta(f)$ implies that $|O \tilde{R}| \leqq |O R|$. Hence

$$w_f(P_0) = |O P_0| / |O Q| = |O R_0| / |O R| \leqq |O P| / |O \tilde{R}| = w_f(P). \square$$

As a consequence we have the following immediate results:

1. Let $n=2$ and let f be as in (2.1). Let $\hat{f}$ be a lifting of f to $\mathbf{C}[x]$ whose coefficients are algebraic integers with positive real parts. Suppose that $\Delta(f) = \Delta(\hat{f})$ and that every face of $\Delta(f)$ that does not contain the origin lies on a line $\alpha_1 X_1 + \alpha_2 X_2 = 1$ with α_1, $\alpha_2 \geqq 0$. If $\hat{f}$ is nondegenerate and commode in the sense of [11], then $\omega(f)$ is the abscissa of convergence of the Dirichlet series ($s \in \mathbf{C}$)

$$Z(f, s) = \sum_{m_1, m_2 \geqq 1} \frac{1}{f(m_1, m_2)^s}$$

studied by Cassou-Nogues [5].

2. Now let n be arbitrary. Let $\hat{f}$ be a quasi-homogeneous polynomial with an isolated singularity at the origin, defined over some number field, and let f be the reduction of $\hat{f}$ modulo some prime ideal. Then $\Delta(\hat{f})$ has only one hyperplane of support $\sum \alpha_i X_i = 1$, and we assume all $\alpha_i \geqq 0$. If we assume that $\Delta(f)$ has dimension n, that $(1, \ldots, 1) \in \mathbf{R}_+ \langle f \rangle$, that $\hat{f}$ is nondegenerate in the sense of [11], and that $\Delta(\hat{f}) = \Delta(f)$, then it follows from Ehlers-Lo [9] * that $\omega(f)$ is the negative of the maximal root of the Bernstein polynomial associated with $\hat{f}$. (The Ehlers-Lo result does not require quasi-homogeneity. This condition is to insure that our definition of Newton polyhedron coincides with theirs.)

At present we do not have an explanation for these apparent connections, other than the fact that they all involve the Newton polyhedron of f in some way. For a relation with the local zeta function of Igusa, see Lichtin-Meuser [12]. Newton polyhedra and local zeta functions are also the topic of a forthcoming paper by J. Denef.

---

* Added in proof. The referee informs us that in the quasi-homogeneous case this result was known before Ehlers-Lo. See I. N. Bernstein (Funct. Anal. and its Appl., Vol. 2, No. 1, 1968, pp. 85-87) and B. Malgrange (Springer Lect. Notes No. 459, pp. 98-119).

REFERENCES

[1] A. ADOLPHSON and S. SPERBER, *Exponential Sums on the Complement of a Hypersurface* (*Amer. J. Math.*, Vol. 102, 1980, pp. 461-487).

[2] A. ADOLPHSON and S. SPERBER, *On the degree of the L-function associated with an exponential sum* (to appear).

[3] A. ADOLPHSON and S. SPERBER, *Newton Polyhedra and the Degree of the L-Function Associated to an Exponential Sum* (*Invent. Math.*, Vol. 88, 1987, pp. 555-569).

[4] J. AX, *Zeroes of Polynomials over Finite Fields* (*Amer. J. Math.*, Vol. 86, 1964, pp. 255-261).

[5] P. CASSOU-NOGUÈS, *Séries de Dirichlet et intégrales associées à un polynôme à deux indéterminées* (*J. of Number Theory*, Vol. 23, 1986, pp. 1-54).

[6] P. DELIGNE, *Cohomologie des intersections complètes* in *Groupes de Monodromie en Géométrie Algébrique* (*SGA 7 II*) (*Lecture Notes in Math.*, No. 340, P. DELIGNE and N. KATZ, pp. 39-61, Berlin-Heidelberg-New York-Tokyo, Springer, 1973).

[7] B. DWORK, *On the Zeta Function of a Hypersurface* (*Publ. Math. I.H.E.S.*, Vol. 12, 1962, pp. 5-68).

[8] B. DWORK, *On the Zeta Function of a Hypersurface, II* (*Ann. of Math.*, Vol. 80, 1964, pp. 227-299).

[9] F. EHLERS and K.-C. LO, *Minimal Characteristic Exponent of the Gauss-Manin Connection of Isolated Singular Point and Newton Polyhedron* (*Math. Ann.*, Vol. 259, 1982, pp. 431-441).

[10] N. KATZ, *On a theorem of Ax* (*Amer. J. Math.*, Vol. 93, 1971, pp. 485-499).

[11] A. G. KOUCHNIRENKO, *Polyèdres de Newton et nombres de Milnor* (*Invent. Math.*, Vol. 32, 1976, pp. 1-31).

[12] B. LICHTIN and D. MEUSER, *Poles of a Local Zeta Function and Newton Polygons* (*Comp. Math.*, Vol. 55, 1985, pp. 313-332).

[13] B. MAZUR, *Frobenius and the Hodge filtration* (*estimates*) (*Ann. of Math.*, Vol. 98, 1973, pp. 58-95).

[14] P. MONSKY, *p-Adic Analysis and Zeta Functions* (*Lectures in Mathematics*, Kyoto University, Tokyo, Kinokuniya Bookstore).

[15] J.-P. SERRE, *Endomorphismes complètement continus des espaces de Banach p-adiques* (*Publ. Math. I.H.E.S.*, Vol. 12, 1962, p. 69-85).

[16] S. SPERBER, *On the p-Adic Theory of Exponential Sums* (*Amer. J. Math.*, Vol. 108, 1986, pp. 255-296).

[17] E. WARNING, *Bemerkung zur vorstehenden Arbeit von Herr Chevalley* (*Abh. Math. Sem. Univ. Hamburg*, Vol. 11, 1936, pp. 76-83).

[18] A. WEIL, *Number of Solutions of Equations in Finite Fields* (*Bull. Amer. Math. Soc., Vol.* 55, 1949, *pp.* 497-508).

(Manuscrit reçu le 25 août 1986,
révisé le 30 mars 1987).

Alan ADOLPHSON,
Department of Mathematics,
Oklahoma State University,
Stillwater, Oklahoma 74078, U.S.A.;

Steven SPERBER,
School of Mathematics,
University of Minnesota,
Minneapolis, Minnesota 55455, U.S.A.