COMPOSITIO MATHEMATICA

A. ADOLPHSON

STEVEN SPERBER

Character sums in finite fields

Compositio Mathematica, tome 52, nº 3 (1984), p. 325-354

<http://www.numdam.org/item?id=CM_1984__52_3_325_0>

Compositio Mathematica 52 (1984) 325–354

CHARACTER SUMS IN FINITE FIELDS

A. Adolphson * and Steven Sperber **

1. Introduction

Let p be a prime, $q = p^a$, and denote by $\boldsymbol{F}_{q^m}$ the field of q^m elements. Let $\chi_1, \dots, \chi_b$: $\boldsymbol{F}_{q^m} \to \boldsymbol{C}^{\times}$ be multiplicative characters. Composing with the norm map N_m: $\boldsymbol{F}_{q^m}^{\times} \to \boldsymbol{F}_q^{\times}$ gives multiplicative characters on $\boldsymbol{F}_{q^m}^{\times}$:

$$\chi_i^{(m)} = \chi_i \circ N_m \colon \boldsymbol{F}_{q^m}^{\times} \to \boldsymbol{C}^{\times}.$$

We extend these characters to $\boldsymbol{F}_{q^m}$ by defining $\chi_i^{(m)}(0) = 0$.

Let X be an algebraic variety over $\boldsymbol{F}_q$ and $\bar{g}_1, \dots, \bar{g}_b$ regular functions on X. We define character sums $S_m(X; \bar{g}_1, \dots, \bar{g}_b; \chi_1, \dots, \chi_b)(= S_m)$ by

$$S_m = \sum \prod_{i=1}^{b} \chi_i^{(m)}(\bar{g}_i(x)), \tag{1.1}$$

where the sum is over all $x \in X(\boldsymbol{F}_{q^m})$, the $\boldsymbol{F}_{q^m}$-valued points of X.

Such sums have been studied classically by Davenport [6] in the one variable case, and the Brewer and Jacobsthal sums in particular are of this type. More recently, mixed sums involving additive and multiplicative characters have been treated p-adically by Gross-Koblitz, Boyarsky, Robba, and Adolphson-Sperber. Sums involving multiplicative characters alone have been studied p-adically by Heiligman, in his Princeton thesis, and by Dwork [10a]. Indeed, the present work is related to Dwork's one-variable cohomological study of sums of this type associated to the hypergeometric differential equation (see [2]).

The L-function associated with these character sums by the formula

$$L(t) = \exp\left(\sum_{m=1}^{\infty} S_m t^m / m \right)$$

---

* Partially supported by NSF grants MCS 79-03315 and MCS81-08814(A01).

** Partially supported by NSF grant MCS 80-01865.

is an Artin L-function associated with a certain Kummer covering of X. More precisely, let ω be a generator for the cyclic group of multiplicative characters of $\boldsymbol{F}_q^\times$ and write $\chi_i = \omega^{\mu_i}$, $i = 1,\dots,b$. The $\boldsymbol{F}_q^\times$-covering Y of X defined by

$$y^{q-1} = \prod_{i=1}^{b} \bar{g}_i(x)^{\mu_i}$$

(where $g \in \boldsymbol{F}_q^\times$ acts on Y by sending (x, y) to (x, gy)) and character ω determine an Artin L-function

$$L\left(X, \prod_{i=1}^{b} \bar{g}_i^{\mu_i}, \omega; t\right) = \prod_P \left(1 - \omega\left(N_{\deg P}\left(\prod_{i=1}^{b} \bar{g}_i(P)^{\mu_i}\right)\right) t^{\deg P}\right)^{-1}, \tag{1.2}$$

where P runs over all closed point of X and $\deg P$ is the degree of the residue field of P over $\boldsymbol{F}_q$. It is well-known that these two constructions agree, i.e.,

$$L(t) = L\left(X, \prod_{i=1}^{b} \bar{g}_i^{\mu_i}, \omega; t\right). \tag{1.3}$$

By results of Dwork and Grothendieck, this L-function is rational. In this article, we are concerned with the case where X is affine space with the coordinate hyperplanes removed and $\bar{g}_1,\dots,\bar{g}_b \in \boldsymbol{F}_q[x_1,\dots,x_n]$. Put

$$S_m^* = \sum \prod_{i=1}^{b} \chi_i^{(m)}(\bar{g}_i(x)), \tag{1.4}$$

where the sum is over all $x = (x_1,\dots,x_n) \in (\boldsymbol{F}_{q^m}^\times)^n$. Let

$$L^*(\bar{g}_1,\dots,\bar{g}_b; \chi_1,\dots,\chi_b; t)(= L^*(t)) = \exp\left(\sum_{m=1}^{\infty} S_m^* t^m/m\right). \tag{1.5}$$

The theory of Dwork and Reich produces a p-adic entire function (of the variable t), namely $\det(I - t\alpha)$, the Fredholm determinant of the completely continuous Frobenius endomorphism α of a certain p-adic Banach space. This entire function is related to $L^*(t)$ (see Eqn. (2.17)). The main result of this paper is Theorem 3, which gives a lower bound for the Newton polygon of $\det(I - t\alpha)$. This lower bound gives useful information concerning the properties and particularly the p-adic behavior of the character sums. In particular, we are able to apply the estimates for the Newton polygon to obtain bounds for the degree and total degree of $L^*(t)$ (where we define for a rational function f/g, f and g relatively prime polynomials,

$$\text{degree}(f/g) = \deg f - \deg g$$

$$\text{total degree}(f/g) = \deg f + \deg.)$$

These results (Theorems 4, 5, 6, 7) may be regarded as the analogues for multiplicative characters of the main theorems of [4] and [5].

We thank the referee for indicating how Deligne's work on the Euler-Poincaré characteristic reduces our computation of the degree of the L-function to the degree of the zeta function of an associated variety. To estimate this degree the results of Bombieri [4] may be applied. However a better result is obtained by modifying his argument. Thus the fine analysis of the entire function $\det(I - t\alpha)$ is not, strictly speaking, necessary for the computation of the degree of $L^*(t)$. However, the estimates for the matrix of the Frobenius endomorphism α and for the Newton polygon of $\det(I - t\alpha)$ enable us to obtain estimates for the total degree of $L^*(t)$ and to analyze the unit roots (Theorem 8) of $L^*(t)$.

We therefore view this paper as constructing the (pre-cohomological) Banach space theory for the p-adic study of the character sums S_m and the associated L-functions $L(t)$. In addition, we draw from the pre-cohomological theory new information concerning degree, total degree, and "first slope" of the Newton polygon. As in other situations of this type, we believe that in the generic case $L^*(t)^{(-1)^{n+1}}$ is a polynomial of degree equal to the upper estimate (namely, D^n) we obtain in Theorem 5 for $\deg L^*(t)^{(-1)^{n+1}}$. We believe that generically $L(t)^{(-1)^{n-1}}$ is a polynomial of degree $(D-1)^n$. The present study indicates a possible weight function which will underlie a Dwork-type cohomological analysis of these character sums.

We believe the methods of this paper will lead to a similar treatment of "mixed" sums of the type

$$\sum_{x \in (F_q^\times)^n} \chi(g(x))\Psi(f(x)),$$

where $f, g \in F_q[x_1, \dots, x_n]$, χ is a multiplicative character on $F_q^\times$, and Ψ is an additive character on F_q.

The outline of the paper is as follows: in Sections 2, 3, 4, 5 we derive the lower bound for the Newton polygon. We apply this result in Section 6 to estimate the degree of $L^*(t)$ and in Section 7 to estimate the total degree of $L^*(t)$. In Section 8 we find sufficient conditions for $L^*(t)$ to have a unique unit root and study the example of an elliptic curve that is a three-fold covering of the line.

Finally, we note that if h_1, h_2 are polynomials and χ a multiplicative character, then

$$\chi(h_1(x)/h_2(x))=\chi(h_1(x))\cdot\chi^{-1}(h_2(x)).$$

Hence by increasing the number b of characters if necessary, our results may be easily extended to the case where $\bar{g}_1,\ldots,\bar{g}_b$ are rational functions.

The first author would like to thank the University of Minnesota for its hospitality while this research was carried out.

2. Theory of Dwork-Reich

In this section we fix notation and review the work of Reich [13]. Let $\boldsymbol{Q}_p$ denote the p-adic numbers and let Ω be the completion of an algebraic closure of $\boldsymbol{Q}_p$. Let K_a denote the unique unramified extension of $\boldsymbol{Q}_p$ in Ω of degree a over $\boldsymbol{Q}_p$. The residue class field of K_a is $\boldsymbol{F}_q$ (where $q=p^a$) and the Frobenius automorphism $x \mapsto x^p$ of $\mathrm{Gal}(\boldsymbol{F}_q/\boldsymbol{F}_p)$ lifts to a generator τ of $\mathrm{Gal}(K_a/\boldsymbol{Q}_p)$. If ζ is a $(q-1)$-st root of unity in K_a, then $\tau(\zeta)=\zeta^p$. Denote by "ord" the additive valuation on Ω normalized so that $\operatorname{ord} p = 1$, and denote by "ord_q" the additive valuation normalized so that $\operatorname{ord}_q q=1$.

Let $\bar{h}\in \boldsymbol{F}_q[x_1,\ldots,x_n]$ be a non-zero homogeneous polynomial of degree $d\geqslant 1$. Let $\mathcal{O}_a$ denote the ring of integers of K_a. We denote by h the polynomial in $\mathcal{O}_a[x_1,\ldots,x_n]$ whose coefficients are roots of unity and whose reduction $\bmod\, p$ is $\bar{h}$ (i.e., h is the Teichmüller lifting of $\bar{h}$).

For technical reasons, in order to apply the results of [13], we work over a field whose value group contains positive rational numbers ϵ, Δ satisfying $\epsilon + d\Delta < 1/q$. For example, taking $\Omega_0 = K_a(\pi)$, where π is a root of p of sufficiently high order, gives such a field. Put $\Omega_1 = \boldsymbol{Q}_p(\pi)$. The Frobenius automorphism τ of K_a is extended to Ω_0 by requiring that $\tau(\pi)=\pi$.

For ϵ, Δ as above, define a subset $\mathscr{D}=\mathscr{D}(\epsilon,\Delta,h)$ of Ω^n by

$$\mathscr{D}(\epsilon,\Delta,h)=\{y=(y_1,\ldots,y_n)\in\Omega^n \mid \operatorname{ord} h(y)\leqslant\epsilon,$$
$$\operatorname{ord} y_i \geqslant -\Delta,\ i=1,\ldots,n\}. \tag{2.1}$$

Denote by $\mathscr{F}=\mathscr{F}(\epsilon,\Delta,h)$ the space of bounded holomorphic functions on $\mathscr{D}(\epsilon,\Delta,h)$ that are defined over Ω_0, i.e., $\mathscr{F}$ is the set of bounded functions on $\mathscr{D}$ that are uniform limits of rational functions in $\Omega_0(x_1,\ldots,x_n)$ whose denominators are non-vanishing on $\mathscr{D}$. Under the sup norm, $\mathscr{F}$ is a p-adic Banach space of type $c(I)$ (in the terminology of [14]). If $\bar{h}$ is a product of distinct irreducible factors, then Reich [13] has given an explicit orthonormal basis for $\mathscr{F}$: The order of the variables $x_1,\ldots,x_n$ induces a lexicographic order on the set of monomials of fixed degree in $x_1,\ldots,x_n$. Let M be the maximal monomial occurring in h. Let

$\{Q_\nu\}_{\nu \geqslant 0}$ be the set of all monomials not divisible by M. Then the set

$$I = \{Q_\nu h^j\}_{\nu \geqslant 0, j \in Z} \tag{2.2}$$

can be made into an orthonormal basis for $\mathscr{F}$ by multiplying each $i \in I$ by a suitable constant $\gamma_i \in \Omega_0$.

Let ψ_p be the Ω-linear endomorphism of $\mathscr{F}$ defined by

$$\psi_p(\xi)(x) = p^{-n} \sum_{y^p = x} \xi(y) \qquad (\text{for } \xi \in \mathscr{F}),$$

where the sum runs over n-tuples $y = (y_1, \ldots, y_n) \in \Omega^n$ such that $y_i^p = x_i$, $i = 1, \ldots, n$, and let $\psi_q = (\psi_p)^a$. For $F \in \mathscr{F}$, we denote by $\alpha_F = \psi_q \circ F$ the endomorphism of $\mathscr{F}$ obtained by composing ψ_q with multiplication by F. Reich [13] shows that α_F is completely continuous (in the sense of [14]), hence the following hold:

Tr α_F and $\det(I - t\alpha_F)$ are well-defined and independent of ϵ, Δ (subject to ϵ, $\Delta > 0$, $\epsilon + d\Delta < 1$). (2.3A)

$$\det(I - t\alpha_F) \text{ is a } p\text{-adic entire function.} \tag{2.3B}$$

$$\det(I - t\alpha_F) = \exp\left(\sum_{m=1}^{\infty} \operatorname{tr}(\alpha_F)^m t^m / m \right). \tag{2.3C}$$

Define for $m \geqslant 1$

$$\mathscr{S}_m = \left\{ x = (x_1, \ldots, x_n) \in \Omega^n | x_i^{q^m - 1} = 1, \quad i = 1, \ldots, n, \bar{h}(\bar{x}) \neq 0 \right\},$$

where $\bar{x} \in (F_{q^m})^n$ is the reduction of x modulo p. The Reich trace formula [13] asserts

$$(q^m - 1)^n \operatorname{tr}(\alpha_F)^m = \sum_{x \in \mathscr{S}_m} F(x) F(x^q) \cdot \ldots \cdot F(x^{q^{m-1}}). \tag{2.4}$$

We now describe how (2.4) connects p-adic analysis with the theory of character sums. Suppose we have b multiplicative characters $\chi_1, \ldots, \chi_b$: $F_q^\times \to K_a^\times$ (we allow one or more of these characters to be trivial). Composing with the norm map N_m: $F_{q^m}^\times \to F_q^\times$ gives multiplicative characters on $F_{q^m}^\times$:

$$\chi_i^{(m)} = \chi_i \circ N_m : F_{q^m}^\times \to K_a^\times,$$

which we extend to F_{q^m} by defining $\chi_i^{(m)}(0) = 0$. Let $\bar{g}_1, \ldots, \bar{g}_b \in$

$\boldsymbol{F}_q[x_1,\ldots,x_n]$ and put $d_i = \deg g_i$. We are interested in the character sum

$$S_m^*(\bar{g}_1,\ldots,\bar{g}_b;\chi_1,\ldots,\chi_b) = \sum_{\bar{x}\in(\boldsymbol{F}_{q^m}^\times)^n} \prod_{i=1}^{b} \chi_i^{(m)}(\bar{g}_i(\bar{x})) \tag{2.5}$$

and its associated L-function

$$L^*(\bar{g}_1,\ldots,\bar{g}_b;\chi_1,\ldots,\chi_b;t)$$
$$= \exp\left(\sum_{m=1}^{\infty} S_m^*(\bar{g}_1,\ldots,\bar{g}_b;\chi_1,\ldots,\chi_b)t^m/m\right). \tag{2.6}$$

We first give an elementary argument to replace the $\bar{g}_i$ by rational functions which are quotients of homogeneous polynomials of the same degree.

For $i = 1,\ldots,b$, let $\hat{g}_i \in \boldsymbol{F}_q[x_0, x_1,\ldots,x_n]$ be the homogenization of $\bar{g}_i$:

$$\hat{g}_i(x_0, x_1,\ldots,x_n) = x_0^{d_i}\bar{g}_i(x_1/x_0,\ldots,x_n/x_0).$$

Then

$$S_m^*(\hat{g}_1/x_0^{d_1},\ldots,\hat{g}_b/x_0^{d_b};\chi_1,\ldots,\chi_b)$$
$$= \sum_{\bar{x}=(x_0,\ldots,x_n)\in(\boldsymbol{F}_{q^m}^\times)^{n+1}} \prod_{i=1}^{b} \chi_i^{(m)}(\hat{g}_i(\bar{x})/x_0^{d_i})$$
$$= \sum_{\bar{x}=(x_0,\ldots,x_n)\in(\boldsymbol{F}_{q^m}^\times)^{n+1}} \prod_{i=1}^{b} \chi_i^{(m)}\left(\bar{g}_i\left(\frac{x_1}{x_0},\ldots,\frac{x_n}{x_0}\right)\right)$$
$$= (q^m - 1)S_m^*(\bar{g}_1,\ldots,\bar{g}_b;\chi_1,\ldots,\chi_b). \tag{2.7}$$

Hence

$$L^*(\hat{g}_1/x_0^{d_1},\ldots,\hat{g}_b/x_0^{d_b};\chi_1,\ldots,\chi_b;t)$$
$$= L^*(\bar{g}_1,\ldots,\bar{g}_b;\chi_1,\ldots,\chi_b;qt)/L^*(\bar{g}_1,\ldots,\bar{g}_b;\chi_1,\ldots,\chi_b;t). \tag{2.8}$$

By factoring the $\hat{g}_i$ into their irreducible factors and using the multiplicativity of the χ_i, we can find distinct irreducible homogeneous polynomials $\bar{h}_1,\dots,\bar{h}_c \in \mathbf{F}_q[x_0, x_1,\dots,x_n]$ and multiplicative characters $\chi_1',\dots,\chi_c'$ such that

$$\begin{aligned} &S_m^*\big(\hat{g}_1/x_0^{d_1},\dots,\hat{g}_b/x_0^{d_b};\chi_1,\dots,\chi_b\big)\\ &\quad= S_m^*\big(\bar{h}_1/x_0^{e_1},\dots,\bar{h}_c/x_0^{e_c};\chi_1',\dots,\chi_c'\big), \end{aligned} \tag{2.9}$$

where $e_i = \deg \bar{h}_i$. Furthermore, $\bar{h}_i$ is not divisible by x_0 for any i.

Thus if we set $\bar{h} = x_0\bar{h}_1\bar{h}_2\cdot\ \dots\ \cdot\bar{h}_c$, then $\bar{h}$ satisfies Reich's hypothesis, namely, $\bar{h}$ is a product of distinct irreducible factors. Let ω: $\mathbf{F}_q^\times \to K_a^\times$ be the Teichmüller character: for $\bar{x}\in\mathbf{F}_q^\times$, $\omega(\bar{x})$ is the unique root of unity in $K_a^\times$ whose reduction mod p is $\bar{x}$. The character group of $\mathbf{F}_q^\times$ is cyclic of order $q-1$, generated by ω, so we may write $\chi_i' = \omega^{\mu_i}$ for $i = 1, 2,\dots,c$, where $0 \leqslant \mu_i \leqslant q-2$. For $i = 1, 2,\dots,c$, set

$$H_i(x) = \big(h_i(x)/x_0^{e_i}\big)\big(h_i(x^q)/h_i(x)^q\big)^{1/(q-1)}, \tag{2.10}$$

where h_i is the Teichmüller lifting of $\bar{h}_i$. Note that $h_i(x^q) = h_i(x)^q + pf_i(x)$, where $f_i(x)\in\mathcal{O}_a[x_0, x_1,\dots,x_n]$ is a homogeneous polynomial of degree qe_i, hence

$$H_i(x) = \big(h_i(x)/x_0^{e_i}\big)\big(1+\big(p\cdot f_i(x)/h_i(x)^q\big)\big)^{1/(q-1)}. \tag{2.11}$$

The second factor on the right may be expanded by the binomial series, and will converge for $|p\cdot f_i(x)/h_i(x)^q| < 1$. It is then straightforward to check that $H_i(x)\in\mathscr{F}(\epsilon, \Delta, h)$ for suitable ϵ, Δ, where $h = x_0\prod_{j=1}^c h_j$.

Note that if $x\in\mathscr{D}(\epsilon, \Delta, h)$ satisfies $x^q = x$, then (2.10) implies $H_i(x)^{q-1} = 1$. Furthermore, for such x, equation (2.11) implies that $H_i(x)$ mod p coincides with $\bar{h}_i(\bar{x})/\bar{x}_0^{e_i}$, where $\bar{x}$ denotes the reduction of x mod p. Hence

$$H_i(x) = \omega\big(\bar{h}_i(\bar{x})/\bar{x}_0^{e_i}\big). \tag{2.12}$$

More generally, if $x\in\mathscr{D}(\epsilon, \Delta, h)$, $x^{q^m} = x$, then

$$\omega\big(N_m\big(\bar{h}_i(\bar{x})/\bar{x}_0^{e_i}\big)\big) = H_i(x)H_i(x^q)\cdot\ \dots\ \cdot H_i\big(x^{q^{m-1}}\big). \tag{2.13}$$

It follows immediately that

$$S_m^*\big(\bar{h}_1/x_0^{e_1},\dots,\bar{h}_c/x_0^{e_c};\chi_1',\dots,\chi_c'\big) = \sum_{x\in\mathscr{S}_m}\prod_{j=0}^{m-1}\prod_{i=1}^{c} H_i\big(x^{q^j}\big)^{\mu_i}. \tag{2.14}$$

Put $H(x)=\prod_{i=1}^{c}H_i(x)^{\mu_i}\in\mathscr{F}(\epsilon,\Delta,h)$ and let α_H denote the composition $\psi_q\circ H$, acting on $\mathscr{F}(\epsilon,\Delta,h)$. We define an operator δ on power series with constant term 1 as follows: if $f(t)\in 1+t\Omega[[t]]$, put $f(t)^\delta = f(t)/f(qt)$. Then (2.3C), (2.4), and (2.14) imply

$$L^*\left(\bar{h}_1/x_0^{e_1},\ldots,\bar{h}_c/x_0^{e_c};\chi_1',\ldots,\chi_c';t\right)^{(-1)^n}=\det(I-t\alpha_H)^{\delta^{n+1}}. \tag{2.15}$$

By (2.8) and (2.9),

$$\begin{aligned}&L^*\left(\bar{h}_1/x_0^{e_1},\ldots,\bar{h}_c/x_0^{e_c};\chi_1',\ldots,\chi_c';t\right)^{-1}\\&\quad=L^*(\bar{g}_1,\ldots,\bar{g}_b;\chi_1,\ldots,\chi_b;t)^{\delta}.\end{aligned} \tag{2.16}$$

The injectivity of δ then allows us to express the original L-function in terms of α_H:

$$L^*(\bar{g}_1,\ldots,\bar{g}_b;\chi_1,\ldots,\chi_b;t)^{(-1)^{n-1}}=\det(I-t\alpha_H)^{\delta^n}. \tag{2.17}$$

This equation is the starting point for our work. We shall estimate the Newton polygon of $\det(I-t\alpha_H)$ (under a certain hypothesis on the χ_i') and use this estimate to study the L-function on the left-hand side of (2.17).

3. A Reduction Step

Our method gives a good estimate for the Newton polygon when all χ_i' take values in $\boldsymbol{Q}_p^\times$. Since $\chi_i'=\omega^{\mu_i}$, this will be the case exactly when

$$\mu_i=\left(1+p+p^2+\ldots+p^{a-1}\right)\nu_i$$

(recall that $q=p^a$), where $0\leqslant\nu_i\leqslant p-2$. This gives a factorization of H: If we put

$$H_0^{(i)}(x)=\left(h_i(x)/x_0^{e_i}\right)\left({}^{\tau}h_i(x^p)/h_i(x)^p\right)^{1/(p-1)},$$

then

$$H_i(x)^{\mu_i}=\prod_{j=0}^{a-1}{}^{\tau^j}H_0^{(i)}\left(x^{p^j}\right)^{\nu_i}. \tag{3.1}$$

Put $\alpha_{H,0}=\psi_p\circ\tau^{-1}\circ\prod_{i=1}^{c}H_0^{(i)}(x)^{\nu_i}$, an Ω_1-linear endomorphism of $\mathscr{F}$.

Equation (3.1) implies

$$\alpha_H = (\alpha_{H,0})^a. \tag{3.2}$$

The Fredholm determinants of α_H and $\alpha_{H,0}$ are related by

$$\det(I - t^a\alpha_H)^a = \prod \det_{\Omega_1}(I - \zeta t\alpha_{H,0}),$$

where the product is over all roots of $\zeta^a = 1$ (see [10, §7]). Thus a point $(x, y) \in \boldsymbol{R}^2$ is a vertex of the Newton polygon of $\det(I - t\alpha_H)$ computed with respect to the valuation "ord_q" if and only if (ax, ay) is a vertex of the Newton polygon of $\det_{\Omega_1}(I - t\alpha_{H,0})$ computed with respect to the valuation "ord." Hence we are reduced to estimating the Newton polygon of $\det_{\Omega_1}(I - t\alpha_{H,0})$, which will be the object of the next two sections.

4. Estimates for the Frobenius Matrix

For our purposes, it is convenient to give a new orthonormal basis for the space $\mathscr{F} = \mathscr{F}(\epsilon, \Delta, h)$, where $h = x_0h_1 \cdot \ldots \cdot h_c$ is a product of distinct irreducible homogeneous polynomials with unit coefficients. We shall define a total order on the set of monomials in $x_0, x_1, \ldots, x_n$. Let M', M'' be two such monomials and denote by $\text{ord}_{x_0}(M')$ (resp. $\text{ord}_{x_0}(M'')$) the highest power of x_0 that divides M' (resp. M'').

1. If $\deg M' < \deg M''$, define $M' < M''$.
2. If $\deg M' = \deg M''$ and $\text{ord}_{x_0}M' > \text{ord}_{x_0}M''$, define $M' < M''$.
3. If $\deg M' = \deg M''$ and $\text{ord}_{x_0}M' = \text{ord}_{x_0}M''(= e$, say),

then $x_0^{-e}M'$ and $x_0^{-e}M''$ are monomials in $x_1, \ldots, x_n$ of the same degree. The order of the variables $x_1, \ldots, x_n$ induces a lexicographic order on monomials of a fixed degree in $x_1, \ldots, x_n$, hence $x_0^{-e}M'$ and $x_0^{-e}M''$ are ordered. We give M' and M'' the induced ordering. This defines a total order on the set of monomials in $x_0, x_1, \ldots, x_n$ which is compatible with multiplication of monomials, i.e., if M', M'', M''' are monomials and $M' < M''$, then $M'M''' < M''M'''$.

Let M_i be the maximal monomial occurring in h_i. Then $M = \prod_{i=1}^c M_i$ is the maximal monomial in $\prod_{i=1}^c h_i$, x_0M is the maximal monomial in h, and $x_0 \nmid M$. Let $\{Q_\nu\}_{\nu \geqslant 0}$ be the set of all monomials in $x_0, x_1, \ldots, x_n$ that are not divisible by x_0M. By Reich [13], the set $I = \{Q_\nu h^j\}_{\nu \geqslant 0, j \in Z}$ can be made into an orthonormal basis for $\mathscr{F}$ by multiplying each element of I by a suitable constant, namely, any constant $\gamma_{\nu,j}$ such that $\|\gamma_{\nu,j}Q_\nu h^j\|_{\mathscr{F}} = 1$.

Theorem 1: *Let $\{R_\mu\}_{\mu \geqslant 0}$ be the set of all monomials in $x_1, \ldots, x_n$ that are not divisible by M. Then the set*

$$I' = \left\{R_\mu x_0^{k_0}(h_1 \cdot \ldots \cdot h_c)^k\right\}_{\mu \geqslant 0, k_0, k \in \boldsymbol{Z}}$$

can be made into an orthonormal basis for $\mathscr{F}$ *by multiplying each element of* I' *by a suitable constant, namely, any constant* $\gamma(\mu, k_0, k)$ *such that* $\|\gamma(\mu, k_0, k)R_\mu x_0^{k_0}(h_1\cdot\ldots\cdot h_c)^k\|_{\mathscr{F}}=1$.

PROOF: Let $\tilde{h}=h_1\cdot\ldots\cdot h_c$. We must show that every $\xi\in\mathscr{F}$ can be written in the form

$$\xi=\sum_{\mu,k_0,k} a(\mu,k_0,k)\gamma(\mu,k_0,k)R_\mu x_0^{k_0}\tilde{h}^k \tag{4.1}$$

with $\{a(\mu, k_0, k)\}$ converging to 0, and that for such a representation of ξ one has $\|\xi\|_{\mathscr{F}}=\sup_{\mu,k_0,k}|a(\mu, k_0, k)|$. We know by Reich that

$$\xi=\sum_{\nu,j} b(\nu,j)\gamma_{\nu,j}Q_\nu h^j, \tag{4.2}$$

with $\{b(\nu,j)\}$ converging to 0. Put $D=\sum_{i=1}^{c}\deg h_i$. Using [13], we have

$$\operatorname{ord}\gamma_{\nu,j}=\begin{cases}\Delta(\deg Q_\nu+j(D+1)) & \text{if } j\geqslant 0\\ \Delta(\deg Q_\nu)-\epsilon j & \text{if } j<0.\end{cases}$$

To describe $\gamma(\mu, k_0, k)$ we distinguish two cases:
If $k\leqslant k_0$, then

$$\operatorname{ord}\gamma(\mu,k_0,k)=\Delta\big(\deg R_\mu+k_0-k\big)+\begin{cases}\Delta(D+1)k & \text{if } k\geqslant 0\\ -k\epsilon & \text{if } k<0.\end{cases} \tag{4.3}$$

If $k>k_0$, then

$$\operatorname{ord}\gamma(\mu,k_0,k)=\Delta\big(\deg R_\mu+(k-k_0)D\big)+\begin{cases}\Delta k_0(D+1) & \text{if } k_0\geqslant 0\\ -k_0\epsilon & \text{if } k_0<0.\end{cases} \tag{4.4}$$

A straightforward calculation using (4.3) and (4.4) shows that for each ν, j we can write

$$Q_\nu h^j=\sum c(\mu,k_0,k;\nu,j)R_\mu x_0^{k_0}\tilde{h}^k \tag{4.5}$$

(a sum over finitely many triples μ, k_0, k) with

$$\operatorname{ord} c(\mu,k_0,k;\nu,j)\gamma_{\nu,j}\gamma(\mu,k_0,k)^{-1}\geqslant 0$$

for all ν, j, μ, k_0, k. Substitution in (4.2) then shows that every $\xi \in \mathscr{F}$ has an expansion of the form (4.1) with $\{a(\mu, k_0, k)\}$ converging to 0.

It remains to show that $\|\xi\|_{\mathscr{F}} = \sup_{\mu,k_0,k}|a(\mu, k_0, k)|$. Clearly, $\|\xi\|_{\mathscr{F}} \leqslant \sup_{\mu,k_0,k}|a(\mu, k_0, k)|$ so we need only prove the opposite inequality. For this, it suffices to show the following.

$$\text{If} \quad \delta > 0 \quad \text{is such that} \quad \|\xi\|_{\mathscr{F}} < \delta, \quad \text{then} \quad \sup_{\mu,k_0,k} |a(\mu, k_0, k)| < \delta. \tag{4.6}$$

For $i = 1, 2$, let

$$\xi_i = \sum\nolimits^{(i)} a(\mu, k_0, k)\gamma(\mu, k_0, k)R_\mu x_0^{k_0}\tilde{h}^k, \tag{4.7}$$

where $\Sigma^{(1)}$ (resp. $\Sigma^{(2)}$) denotes a sum over those μ, k_0, k such that $|a(\mu, k_0, k)| < \delta$ (resp. $|a(\mu, k_0, k)| \geqslant \delta$). Then $\xi = \xi_1 + \xi_2$ and $\|\xi_1\|_{\mathscr{F}} < \delta$, so $\|\xi_2\|_{\mathscr{F}} < \delta$ also. Furthermore, $\Sigma^{(2)}$ is a finite sum since $\{a(\mu, k_0, k)\}$ converges to zero.

For any triple (μ, k_0, k),

$$R_\mu x_0^{k_0}\tilde{h}^k = \sum d(\nu, j;\ \mu, k_0, k)Q_\nu h^j, \tag{4.8}$$

a sum over finitely many pairs ν, j, with $|d(\nu, j;\ \mu, k_0, k)| \leqslant 1$. Furthermore, if we put $\kappa = \min(k_0, k)$, then $d(\nu, j;\ \mu, k_0, k) = 0$ for $j < \kappa$. And if we pick ν' such that

$$Q_{\nu'} = \begin{cases} R_\mu x_0^{k_0-k} & \text{if} \quad \kappa = k \\ R_\mu M^{k-k_0} & \text{if} \quad \kappa = k_0, \end{cases} \tag{4.9}$$

then $|d(\nu', \kappa;\ \mu, k_0, k)| = 1$. Note also that $Q_{\nu'}$ is maximal (in the ordering defined at the beginning of this section) among those monomials Q_ν such that $d(\nu, \kappa;\ \mu, k_0, k) \neq 0$. Finally, note that if ν, j is such that $d(\nu, j;\ \mu, k_0, k) \neq 0$, then

$$\operatorname{ord} \gamma(\mu, k_0, k) \geqslant \operatorname{ord} \gamma_{\nu,j}$$

with equality holding if $(\nu, j) = (\nu', \kappa)$. Consequently,

$$\gamma(\mu, k_0, k)R_\mu x_0^{k_0}\tilde{h}^k = \sum \tilde{d}(\nu, j;\ \mu, k_0, k)\gamma_{\nu,j}Q_\nu h^j, \tag{4.10}$$

where $|\tilde{d}(\nu, j;\ \mu, k_0, k)| \leqslant 1$ and $|\tilde{d}(\nu', \kappa;\ \mu, k_0, k)| = 1$.

Let $\lambda = \min\{\kappa | \kappa = \min(k_0, k),\ |a(\mu, k_0, k)| \geqslant \delta\}$. Consider (4.7) with $i = 2$ and substitute on the right-hand side from (4.10). This expresses ξ_2

in terms of the $\gamma_{\nu,j}Q_\nu h^j$. Choose ρ such that Q_ρ is maximal among all monomials Q_ν such that $Q_\nu h^\lambda$ occurs with non-zero coefficient in this expansion of ξ_2. It is not hard to see that there is a unique triple (μ, k_0, k) such that $|a(\mu, k_0, k)| \geqslant \delta$ and such that $Q_\rho h^\lambda$ occurs with non-zero coefficient on the right-hand side of (4.10), and that $|\tilde{d}(\rho, \lambda; \mu, k_0, k)| = 1$. It then follows that the coefficient of $\gamma_{\rho,\lambda}Q_\rho h^\lambda$ in ξ_2 is $a(\mu, k_0, k)d(\rho, \lambda; \mu, k_0, k)$, which has magnitude $\geqslant \delta$. But $\{\gamma_{\nu,j}Q_\nu h^j\}$ is an orthonormal basis for $\mathscr{F}$, so $\|\xi_2\|_{\mathscr{F}} \geqslant \delta$, a contradiction. This contradiction shows there is no triple μ, k_0, k with $|a(\mu, k_0, k)| \geqslant \delta$, which establishes (4.6). QED

We now return to the problem of estimating the Newton polygon of $\det_{\Omega_1}(I - t\alpha_{H,0})$. Let $\xi_1, \dots, \xi_a$ be an integral basis for Ω_0 over Ω_1 that has the property of p-adic directness [9, §3c], i.e., for any $\beta_1, \dots, \beta_a \in \Omega_1$,

$$\operatorname{ord}\left(\sum_{j=1}^{a} \beta_j \xi_j\right) = \min_j\left(\operatorname{ord} \beta_j\right).$$

Then an orthonormal basis for $\mathscr{F}$ as an Ω_1-linear space can be obtained from the set

$$\tilde{I} = \left\{\xi_l R_\mu x_0^{k_0} \tilde{h}^k\right\}_{1 \leqslant l \leqslant a, \mu \geqslant 0, k_0, k \in Z}$$

by multiplying each $i \in \tilde{I}$ by a suitable constant $\gamma_i \in \Omega_0$ (in fact, one may take $\gamma_i = \gamma(\mu, k_0, k)$ as given by (4.3) and (4.4)).

Put $e_i = \deg h_i$ for $i = 1, \dots, c$, let $E = \sum_{i=1}^{c} e_i \nu_i$ and let $R = [E/(p-1)]$, where the ν_i are as defined in §3. Let $\deg(R_\mu x_0^{k_0}\tilde{h}^k)$ denote the degree of $R_\mu x_0^{k_0}\tilde{h}^k$ as rational function (i.e., degree of numerator minus degree of denominator). A straightforward calculation using the definition of $\alpha_{H,0}$ shows that if $\xi_l R_\mu x_0^{k_0}\tilde{h}^k \in \tilde{I}$, then all basis elements $\xi_{l'} R_{\mu'} x_0^{k_0'}\tilde{h}^{k'} \in \tilde{I}$ that appear with non-zero coefficient in $\alpha_{H,0}(\xi_l R_\mu x_0^{k_0}\tilde{h}^k)$ satisfy

$$\deg\left(R_{\mu'} x_0^{k_0'}\tilde{h}^{k'}\right) = \deg\left(R_\mu x_0^{k_0}\tilde{h}^k\right)/p \tag{4.11}$$

$$k_0' \geqslant (k_0 - E)/p. \tag{4.12}$$

Let $\mathscr{F}_J$ be the closed Ω_1-subspace of $\mathscr{F}$ with orthonormal basis

$$J = \left\{\xi_l R_\mu x_0^{k_0}\tilde{h}^k \in \tilde{I} \middle| \deg\left(R_\mu x_0^{k_0}\tilde{h}^k\right) = 0 \quad \text{and} \quad k_0 \geqslant -R\right\}.$$

Then (4.11) and (4.12) imply that $\alpha_{H,0}$ is stable on $\mathscr{F}_J$, so by [14, Lemme 2],

$$\det_{\Omega_1}(I - t\alpha_{H,0}|\mathscr{F}) = \det_{\Omega_1}(I - t\alpha_{H,0}|\mathscr{F}_J)\det_{\Omega_1}(I - t\alpha_{H,0}|\mathscr{F}/\mathscr{F}_J). \tag{4.13}$$

But (4.11) implies that $|\deg(R_{\mu'}x_0^{k_0'}\tilde{h}^{k'})| < |\deg(R_\mu x_0^{k_0}\tilde{h}^k)|$ unless $\deg R_\mu x_0^{k_0}\tilde{h}^k = 0$, and (4.12) implies that $k_0 < k_0'$ unless $k_0 \geqslant -R$. Hence by [14, Prop. 12]

$$\det_{\Omega_1}(I - t\alpha_{H,0}|\mathscr{F}/\mathscr{F}_J) = 1. \tag{4.14}$$

Equations (4.13) and (4.14) reduce us to the problem of estimating the Newton polygon of $\det_{\Omega_1}(I - t\alpha_{H,0}|\mathscr{F}_J)$. Let

$$\det_{\Omega_1}(I - t\alpha_{H,0}|\mathscr{F}_J) = \sum_{m=0}^{\infty} c_m t^m. \tag{4.15}$$

For $i = \xi_\iota R_\mu x_0^{k_0}\tilde{h}^k \in J$, put

$$\alpha_{H,0}(i) = \sum_{i'\in J} C(i,i')i',$$

so that $(C(i,i'))_{i,i'\in J}$ is the matrix of $\alpha_{H,0}$ with respect to J. By [14, Prop. 7a],

$$c_m = (-1)^m \sum \sum_{\sigma} \operatorname{sgn}(\sigma) C(i_1, i_{\sigma(1)}) \cdot \ldots \cdot C(i_m, i_{\sigma(m)}), \tag{4.16}$$

where the outer sum is over all subsets $\{i_1,\ldots,i_m\}$ of m distinct elements of J and the inner sum is over all permutations σ on m letters, $\operatorname{sgn}(\sigma)$ being the sign of the permutation σ. The main result of this section is Theorem 2, which estimates ord $C(i, i')$. In the next section we shall use (4.15), (4.16), and Theorem 2 to estimate the Newton polygon of $\det_{\Omega_1}(I - t\alpha_{H,0}|\mathscr{F}_J)$.

For $j \in \boldsymbol{Z}$, $j \leqslant 0$, put

$$\lambda(j) = \left[\frac{-j-1}{p}\right] + 1, \tag{4.17}$$

i.e., $\lambda(j)$ is the smallest integer such that $p\lambda(j) + j \geqslant 0$. For convenience we put $\lambda(j) = 0$ when $j > 0$. Define

$$\nu = \min_{\iota=1,\ldots,c} \{\nu_\iota\}.$$

Theorem 2: *If* $i = \xi_\iota R_\mu x_0^{k_0}\tilde{h}^k \in J$, $i' = \xi_{\iota'} R_{\mu'} x_0^{k_0'}\tilde{h}^{k'} \in J$, *then*

$$\operatorname{ord} C(i,i') \geqslant \max\{0, -k' - \lambda(k+\nu)\}. \tag{4.18}$$

Proof: Put ${}^{\tau}h_\iota(x^p) = h_\iota(x)^p + pf_\iota(x)$, where $f_\iota \in \mathcal{O}_a[x]$ has degree pe_ι.

Then

$$\begin{aligned} H_0^{(\iota)}(x)^{\nu_\iota} &= \left(h_\iota(x)/x_0^{e_\iota}\right)^{\nu_\iota}\left({}^{\tau}h_\iota(x^p)/h_\iota(x)^p\right)^{\nu_\iota/(p-1)} \\ &= \left(h_\iota(x)/x_0^{e_\iota}\right)^{\nu_\iota}\left(1+\frac{pf_\iota(x)}{h_\iota(x)^p}\right)^{\nu_\iota/(p-1)} \\ &= \frac{h_\iota(x)^{\nu_\iota}}{x_0^{e_\iota\nu_\iota}}\sum_{r=0}^{\infty} a_r^{(\iota)}B_r^{(\iota)}(x)h_\iota(x)^{-rp}, \end{aligned} \tag{4.19}$$

where $a_r^{(\iota)} \in \mathcal{O}_a$ satisfies $a_0^{(\iota)} = 1$ and $\operatorname{ord} a_r^{(\iota)} \geqslant r$ and $B_r^{(\iota)}(x) \in \mathcal{O}_a[x]$ satisfies $B_0^{(\iota)}(x) = 1$, and $\deg B_r^{(\iota)}(x) = e_\iota rp$. Hence

$$\prod_{\iota=1}^{c} H_0^{(\iota)}(x)^{\nu_\iota} = \frac{\prod_{\iota=1}^{c} h_\iota^{\nu_\iota}}{x_0^E}\sum_{r=0}^{\infty} a_r B_r(x)\tilde{h}(x)^{-rp},$$

where $a_r \in \mathcal{O}_a$ satisfies $a_0 = 1$ and

$$\operatorname{ord} a_r \geqslant r \tag{4.20}$$

and $B_r(x) \in \mathcal{O}_a[x]$ satisfies $B_0(x) = 1$ and

$$\deg B_r(x) = \mathrm{D}rp, \tag{4.21}$$

where $D = \sum_{\iota=1}^{c} e_\iota$. Let $H = (\prod_{\iota=1}^{c} h_\iota^{\nu_\iota})/\tilde{h}^{\nu}$.

By [3, Lemma 1]

$$\begin{aligned} \alpha_{H,0}(i) &= \psi_p \circ \tau^{-1}\left(\sum_{r=0}^{\infty} \xi_l a_r B_r(x) R_\mu H x_0^{k_0 - E}\tilde{h}^{k+\nu-rp}\right) \\ &= \psi_p \circ \tau^{-1}\left(\xi_l R_\mu H x_0^{k_0-E}\tilde{h}^{k+\nu}\right) \\ &\quad + \sum_{r=1}^{\infty} a_r \tilde{h}^{-\lambda(k+\nu-rp)}\sum_{s=0}^{\infty} p^s M(l,\mu,k_0,k,r,s)\tilde{h}^{-s}, \end{aligned} \tag{4.22}$$

where $M(l, \mu, k_0, k, r, s) \in \mathcal{O}_a[x_0, x_1, \ldots, x_n, x_0^{-1}]$ satisfies

$$\deg M(l,\mu,k_0,k,r,s) = (\lambda(k+\nu-rp)+s)D. \tag{4.23}$$

Note that $i \in J$ implies $k \leqslant 0$; also, $\nu \leqslant p-2$, so $k+\nu-rp < 0$ for $r \geqslant 1$. We have separated the term where $r = 0$ for special consideration because $k+\nu$ may be positive or negative, and these two cases are treated differently. We can write

$$M(l, \mu, k_0, k, r, s) = \sum_{\alpha, \beta_0, \beta} A(l, \mu, k_0, k, r, s, \alpha, \beta_0, \beta) R_\alpha x_0^{\beta_0} \tilde{h}^\beta$$

with α, $\beta \geqslant 0$, $\beta_0 \geqslant -R$, $\operatorname{ord} A(l, \ldots, \beta) \geqslant 0$, and

$$\deg R_\alpha x_0^{\beta_0} \tilde{h}^\beta = (\lambda(k + \nu - rp) + s) D.$$

Suppose first $k + \nu \geqslant 0$. Then $\psi_p \circ \tau^{-1}(\xi_l R_\mu H x_0^{k_0 - E} \tilde{h}^{k+\nu})$ is an element of $\mathcal{O}_a[x_0, \ldots, x_n, x_0^{-1}]$ and every term on the right-hand side of (4.22) has coefficients in $\mathcal{O}_a$, so we have by p-adic directness the trivial estimate

$$\operatorname{ord} C(i, i') \geqslant 0. \tag{4.24}$$

When $k' = 0$, a short calculation shows that the right-hand side of (4.17) is 0. For $k' < 0$, the coefficient of $R_{\mu'} x_0^{k_0'} \tilde{h}^{k'}$ on the right-hand side of (4.22) is

$$\sum a_r p^s A(l, \mu, k_0, k, r, s, \mu', k_0', \beta), \tag{4.25}$$

where the sum is over $r \geqslant 1$, $s \geqslant 0$, $\beta \in \mathbf{Z}_{\geqslant 0}$ subject to the condition

$$\beta - s - \lambda(k + \nu - rp) = k'. \tag{4.26}$$

Thus by (4.19), (4.25), and the p-adic directness of $\{\xi_l\}_{l=1}^a$,

$$\operatorname{ord} C(i, i') \geqslant \operatorname{Inf}\{r + s\}, \tag{4.27}$$

where the infimum is over all r, s subject to (4.26). Since $\lambda(k + \nu - rp) = r + \lambda(k + \nu)$ and $\beta \geqslant 0$, (4.26) implies

$$r + s \geqslant -k' - \lambda(k + \nu).$$

The theorem now follows immediately from (4.27) and (4.24).

In case $k + \nu < 0$, we have in place of (4.22)

$$\alpha_{H,0}(i) = \sum_{r=0}^{\infty} a_r \tilde{h}^{-\lambda(k+\nu-rp)} \sum_{s=0}^{\infty} p^s M(l, \mu, k_0, k, r, s) \tilde{h}^{-s},$$

where $M(l, \mu, k_0, k, r, s) \in \mathcal{O}_a[x_0, \ldots, x_n, x_0^{-1}]$ satisfies (4.23). One then proceeds as in the case $k + \nu \geqslant 0$, $k' < 0$ using (4.25) and (4.26). QED

5. Weights and the Newton Polygon

Let Γ_m denote the class of subsets of J of cardinality m. We shall define a function w: $J \to \{0\} \cup \{\nu/(p-1) + \boldsymbol{Z}_{\geqslant 0}\}$ (which we shall call a weight function) having the properties that (for c_m as in (4.15))

$$\operatorname{ord} c_m \geqslant \frac{p-1}{p} \inf_{\gamma \in \Gamma_m} \left(\sum_{i \in \gamma} w(i) \right) \tag{5.1}$$

and that for $r \geqslant 0$, the number of $i \in J$ with $w(i) = r$ is finite. Then the problem of estimating ord c_m is reduced to the problem of determining the number of elements of J of a given weight. For $r \in \boldsymbol{Z}_{\geqslant 0}$, define

$$W(0) = a^{-1} \operatorname{card}\{ i \in J | w(i) = 0\}$$

$$W\left(r + \frac{\nu}{p-1}\right) = a^{-1} \operatorname{card}\left\{ i \in J | w(i) = r + \frac{\nu}{p-1}\right\}.$$

The argument of [10, §7] then proves that the Newton polygon of $\det_{\Omega_1}(I - t\alpha_{H,0})$ (with respect to the valuation "ord") lies above the polygon with vertices (0, 0), $(aW(0), 0)$, and (if $\nu > 0$)

$$\left(a\left(W(0) + \sum_{r=0}^{N} W\left(r + \frac{\nu}{p-1}\right)\right),\right.$$

$$\left. a\frac{p-1}{p} \sum_{r=0}^{N} \left(r + \frac{\nu}{p-1}\right) W\left(r + \frac{\nu}{p-1}\right)\right), N = 0, 1, 2, \ldots$$

(if $\nu = 0$ the x-coordinate is replaced by $a\,\Sigma_{r=0}^{N} W(r)$). The last paragraph of §3 then implies

THEOREM 3: *Suppose the* χ_i', $i = 1, 2, \ldots, c$ *all have order dividing* $p-1$. *Then the Newton polygon of* $\det(I - t\alpha_H)$ (*with respect to the valuation* "ord_q") *is contained in the convex closure of the points* (0, 0), $(W(0), 0)$, *and* (*if* $\nu > 0$)

$$\left(W(0) + \sum_{r=0}^{N} W\left(r + \frac{\nu}{p-1}\right),\right.$$

$$\left. \frac{p-1}{p} \sum_{r=0}^{N} \left(r + \frac{\nu}{p-1}\right) W\left(r + \frac{\nu}{p-1}\right)\right), N = 0, 1, 2, \ldots$$

(*if* $\nu = 0$, *the x-coordinate is replaced by* $\Sigma_{r=0}^{N} W(r)$).

It remains to define a weight function w satisfying (5.1).

Lemma 1: *Consider l sequences of real numbers, each of length m: $\{n_r^{(i)}\}_{r=1}^m$, $i=1,2,\dots,l$. Let σ be a permutation on m letters. If x and y are non-negative real numbers, then*

$$\sum_{r=1}^{m}\max_i\left\{xn_{\sigma(r)}^{(i)}-yn_r^{(i)}\right\}\geqslant(x-y)\sum_{r=1}^{m}\max_i\left\{n_r^{(i)}\right\}.$$

Proof: We first show that for any fixed r,

$$\max_i\left\{xn_{\sigma(r)}^{(i)}-yn_r^{(i)}\right\}\geqslant x\max_i\left\{n_{\sigma(r)}^{(i)}\right\}-y\max_i\left\{n_r^{(i)}\right\}. \tag{5.2}$$

Let i_0, i_1 be such that $n_{\sigma(r)}^{(i_0)}=\max_i\{n_{\sigma(r)}^{(i)}\}$, $n_r^{(i_1)}=\max_i\{n_r^{(i)}\}$. Inequality (5.2) follows from the observation that (since $x, y\geqslant 0$)

$$xn_{\sigma(r)}^{(i_0)}-yn_r^{(i_0)}\geqslant xn_{\sigma(r)}^{(i_0)}-yn_r^{(i_1)}.$$

The lemma now follows by summing (5.2) over r. QED

We define a mapping $k\colon J\to\boldsymbol{Z}$ as follows. If $i=\xi_l R_\mu x_0^{k_0}x^k\in J$, put $k(i)=k$.

Proposition 1: *The function*

$$w(i)=\max\left\{0,\ -\left(k(i)+1-\frac{\nu}{p-1}\right)\right\} \tag{5.3}$$

satisfies (5.1).

Proof: From (4.16) and Theorem 2,

$$\operatorname{ord}c_m\geqslant\inf\sum_{r=1}^{m}\max\left\{0,\ -k\left(i_{\sigma(r)}\right)-\lambda\left(k(i_r)+\nu\right)\right\}, \tag{5.4}$$

where the inf is taken over all $\{i_r\}_{r=1}^m\in\Gamma_m$ and over all permutations σ of m letters. From the definition of λ,

$$\lambda(k+\nu)\leqslant-\frac{k}{p}+\left(1-\frac{1+\nu}{p}\right),$$

so (5.4) implies

$$\operatorname{ord}c_m\geqslant p^{-1}\inf\sum_{r=1}^{m}\max\left\{\begin{matrix}0,\ -p\left(k\left(i_{\sigma(r)}\right)+1-\dfrac{\nu}{(p-1)}\right)\\ +\left(k(i_r)+1-\dfrac{\nu}{(p-1)}\right)\end{matrix}\right\}.$$

Now apply Lemma 1 with $l = 2$, $n_r^{(1)} = 0$, $n_r^{(2)} = -(k(i_r) + 1 - \nu/(p-1))$, $x = p$, $y = 1$ to conclude

$$\operatorname{ord} c_m \geqslant \frac{p-1}{p} \inf \sum_{r=1}^{m} \max\left\{0,\ -\left(k(i_r) + 1 - \frac{\nu}{p-1}\right)\right\}. \quad \text{QED}$$

It is now easy to check tht $W(r + \nu/(p-1))$ is a finite rational number. In fact, since $w(\xi_l R_\mu x_0^{k_0} \tilde{h}^k)$ is independent of l, $W(r + \nu/(p-1))$ is an integer. We can determine $W(r + \nu/(p-1))$ explicitly. Let $c(r) = \binom{r+n-1}{n-1}$, the number of monomials of degree r in n variables.

PROPOSITION 2: *Let* $D = \sum_{l=1}^{c} \deg h_l$. *If* $\nu > 0$, *then*

(*i*) $W(0) = \sum_{s=0}^{R} c(s)$

(*ii*) $W(r + \nu/(p-1)) = \sum_{s=rD+R+1}^{(r+1)D+R} c(s)$, $r = 0, 1, 2, \ldots$

If $\nu = 0$, *then*

(*iii*) $W(0) = \sum_{s=0}^{D+R} c(s)$

(*iv*) $W(r) = \sum_{s=rD+R+1}^{(r+1)D+R} c(s)$, $r = 1, 2, 3, \ldots$

PROOF: Suppose $\nu > 0$. Recall that $i \in J$ implies $k(i) \leqslant 0$. By Proposition 1, $w(i) = 0$ if and only if $k(i) = 0$. But $i = \xi_l R_\mu x_0^{k_0} \in J$ implies $k_0 \geqslant -R$ and $\deg(i) = 0$. Thus $W(0)$ is the number of monomials R_μ, not divisible by M, with $\deg R_\mu \leqslant R$. Since $\deg M = D > R$, this is just the number of monomials of degree $\leqslant R$ in n variables, namely, $\sum_{s=0}^{R} c(s)$.

For $r \geqslant 0$, $w(i) = r + \nu/(p-1)$ if and only if $k(i) = -r-1$. Hence $w(r + \nu/(p-1))$ is the number of monomials R_μ, not divisible by M, with $\deg R_\mu \leqslant (r+1)D + R$ (since $k_0 \geqslant -R$). The number of monomials of degree s not divisible by M is $c(s) - c(s-D)$ (we define $c(s) = 0$ for $s < 0$), hence

$$W\left(r + \frac{\nu}{p-1}\right) = \sum_{s=0}^{(r+1)D+R} (c(s) - c(s-D))$$

$$= \sum_{s=rD+R+1}^{(r+1)D+R} c(s).$$

The case $\nu = 0$ is handled similarly. QED

6. Degree of the L-function

By (2.17) and the Dwork rationality criterion [8, Thm. 3], $L^*(\bar{g}_1, \ldots, \bar{g}_b; \chi_1, \ldots, \chi_b; t)^{(-1)^{n-1}}$ is a rational function. Thus we may write

$$L^*(\bar{g}_1,\ldots,\bar{g}_b;\ \chi_1,\ldots,\chi_b;\ t)^{(-1)^{n-1}} = \prod_{i=1}^{r}(1-\rho_i t)\Big/\prod_{j=1}^{s}(1-\eta_j t) \tag{6.1}$$

(so $\deg L^*(\bar{g}_1,\ldots,\bar{g}_b;\ \chi_1,\ldots,\chi_b;\ t)^{(-1)^{n-1}} = r-s$). Inverting (2.17) and solving for the Fredholm determinant of α_H yields

$$\det(I - t\alpha_H) = D_1(t)/D_2(t),$$

where

$$D_1(t) = \prod_{i=1}^{r}\prod_{m=0}^{\infty}(1-q^m\rho_i t)^{c(m)}$$

$$D_2(t) = \prod_{j=1}^{s}\prod_{m=0}^{\infty}(1-q^m\eta_j t)^{c(m)}.$$

Lemma 2 [4, *Corollary to Lemma* 3]: *If* $L^*(g_1,\ldots,g_b;\ \chi_1,\ldots,\chi_b;\ t)^{(-1)^{n-1}}$ *is written as in* (6.1), *then*

$$\begin{aligned}&\sum_{i=1}^{r}\sum{}'\big(x-\operatorname{ord}_q(q^m\rho_i)\big)c(m) - \sum_{j=1}^{s}\sum{}'\big(x-\operatorname{ord}_q(q^m\eta_j)\big)c(m)\\ &\quad\leqslant x\left(W(0) + \sum_{k\leqslant\frac{px-\nu}{p-1}} W\Big(k+\frac{\nu}{p-1}\Big)\right)\\ &\quad\quad - \frac{p-1}{p}\sum_{k\leqslant\frac{px-\nu}{p-1}}\Big(k+\frac{\nu}{p-1}\Big)W\Big(k+\frac{\nu}{p-1}\Big)\end{aligned} \tag{6.2}$$

provided $\nu > 0$, *where the sums* Σ' *are over all* m *such that the summands are positive. If* $\nu = 0$, *the right hand side should be replaced by*

$$x\left(\sum_{k\leqslant px/(p-1)} W(k)\right) - \frac{p-1}{p}\sum_{k\leqslant px/(p-1)} kW(k).$$

Since $\operatorname{ord}_q(q^m\rho_i) = m + \operatorname{ord}_q\rho_i$ and

$$\sum_{m\leqslant x}(x-m)c(m) = x^{n+1}/(n+1)! + \mathcal{O}(x^n)$$

as $x \to +\infty$, the left-hand side of (6.2) equals

$$(r-s)x^{n+1}/(n+1)! + \mathcal{O}(x^n). \tag{6.3}$$

We now determine the asymptotic growth of the right-hand side of (6.2).

PROPOSITION 3: *The right-hand side of* (6.2) *equals*

$$\left(\frac{pD}{p-1}\right)^n \frac{x^{n+1}}{(n+1)!} + \mathcal{O}(x^n).$$

PROOF: We give the proof when $\nu > 0$, the case $\nu = 0$ being similar. By Proposition 2, $W(k+\nu/(p-1))$ is a polynomial in $k+\nu/(p-1)$ of degree $n-1$ with leading coefficient $D^n/(n-1)!$ Hence

$$x\left(W(0) + \sum_{k \leqslant \frac{px-\nu}{p-1}} W\left(k + \frac{\nu}{p-1}\right)\right) \leqslant \left(\frac{pD}{p-1}\right)^n \frac{x^{n+1}}{n!} + \mathcal{O}(x^n)$$

and

$$\sum_{k \leqslant \frac{px-\nu}{p-1}} \frac{p-1}{p}\left(k + \frac{\nu}{p-1}\right) W\left(k + \frac{\nu}{p-1}\right)$$

$$= \left(\frac{Dp}{p-1}\right)^n \frac{x^{n+1}}{(n+1)(n-1)!} + \mathcal{O}(x^n).$$

The proposition follows immediately. QED

We can now estimate the degree of L^*.

THEOREM 4: *Suppose the* χ_i', $i = 1, 2, \ldots, c$ *all have order dividing* $p-1$. *Then*

$$0 \leqslant \deg L^*(\bar{g}_1, \ldots, \bar{g}_b; \chi_1, \ldots, \chi_b; t)^{(-1)^{n-1}} \leqslant \left(\frac{p}{p-1}\right)^n D^n.$$

PROOF: Substituting (6.3) and Proposition 3 into (6.2) and letting $x \to +\infty$ gives the inequality on the right. The inequality on the left follows by the argument of [4, Theorem 1(ii)]. QED

REMARK: Let us drop for a moment the assumption that the χ_i's take values in $\mathbb{Q}_p$. Associated to the collections $\{\bar{g}_i\}_{i=1}^b$, $\{\chi_i\}_{i=1}^b$ is a lisse rank one l-adic ($l \neq p$) étale sheaf $\mathscr{L}$ on the variety $X = \mathbb{A}^n_{\mathbb{F}_q} -$

$\{\prod_{i=1}^{n} x_i \prod_{j=1}^{b} \bar{g}_j(x_1,\dots,x_n)=0\}$. This sheaf has the property that

$$L^*(\bar{g}_1,\dots,\bar{g}_b;\chi_1,\dots,\chi_b;t)=\prod_{i=0}^{2n}\det\left(I-tF|H_c^i(X,\mathscr{L})\right)^{(-1)^{i+1}},$$

where $H_c^i(X,\mathscr{L})$ is étale cohomology with proper supports and F is the Frobenius endomorphism. Hence deg L^* is the Euler-Poincaré characteristic of $\mathscr{L}$. However, $\mathscr{L}$ becomes trivial on an étale galois covering of X of degree prime to p, so by a theorem of Deligne [12], the degree of $L^*(\bar{g}_1,\dots,\bar{g}_b;\chi_1,\dots,\chi_b;t)$ is unchanged if we replace all the χ_i by the trivial character. But Theorem 4 is applicable if all the χ_i are trivial. Thus we have the following more general form of Theorem 4.

THEOREM 5: *For arbitrary multiplicative characters* χ_i *of* $\boldsymbol{F}_q^{\times}$,

$$0\leqslant \deg L^*(\bar{g}_1,\dots,\bar{g}_b;\chi_1,\dots,\chi_b;t)^{(-1)^{n-1}}\leqslant\left(\frac{p}{p-1}\right)^n D^n.$$

In fact, by Deligne's result we have

$$\deg L^*(\bar{g}_1,\dots,\bar{g}_b;\chi_1,\dots,\chi_b;t)=\deg Z(X,t),$$

where $Z(X,t)$ is the zeta function of X. An alternative approach to the problem of bounding $\deg L^*(t)$ is to express $Z(X,t)$ in terms of exponential sums and use the estimates of Bombieri [4]. If we let Ψ be a non-trivial additive character on $\boldsymbol{F}_q$ and put

$$S_m(\Psi)=\sum_{x_0,x_1,\dots,x_n\in \boldsymbol{F}_{q^m}^{\times}}\Psi\left(\mathrm{Tr}_{\boldsymbol{F}_{q^m}/\boldsymbol{F}_q}\left(x_0\prod_{j=1}^{b}\bar{g}_j(x_1,\dots,x_n)\right)\right)$$

$$L^*\left(\Psi,x_0\prod_{j=1}^{b}\bar{g}_j;t\right)=\exp\left(\sum_{m=1}^{\infty}S_m(\Psi)t^m/m\right),$$

then a straightforward combinatorial argument shows

$$Z(X,qt)=(1-t)^{\delta^{n+1}}/L^*\left(\Psi,x_0\prod_{j=1}^{b}\bar{g}_j;t\right),$$

hence

$$\deg Z(X,t)=-\deg L^*\left(\Psi,x_0\prod_{j=1}^{b}\bar{g}_j;t\right).$$

Bombieri's estimate for deg $L^*(\Psi,\ x_0\prod_{j=1}^{b}\bar{g}_j;\ t)$ is not as sharp as Theorem 5. However, one can modify the argument of [4] to take account of the special role played by the variable x_0. This leads to the sharper result:

THEOREM 5′: *For arbitrary multiplicative characters* χ_i, $i = 1,\dots,b$, *of* $\boldsymbol{F}_q^{\times}$,

$$0 \leqslant \deg L^*(\bar{g}_1,\dots,\bar{g}_b;\ \chi_1,\dots,\chi_b;\ t)^{(-1)^{n-1}} \leqslant D^n.$$

More generally, this modification leads to better bounds for the degree (and total degree) of the L-function associated to an exponential sum on a closed subvariety of $\boldsymbol{A}^n$. We intend to report on this result in a subsequent article.

We believe that the upper bound D^n for $L^*(t)^{(-1)^{n-1}}$ (given by Theorem 5′) is best possible and, in fact, is generically attained. Suppose for a moment that $b=1$, i.e., that we have a single polynomial $\bar{g}(x_1,\dots,x_n)$ and a single multiplicative character χ. We believe that if $\bar{g}$ is regular (i.e., the polynomials $\bar{g}$, $x_i(\partial\bar{g}/\partial x_i)$, $i=1,\dots,n$ have no common zero in projective space) and χ is non-trivial, then $L^*(\bar{g};\ \chi;\ t)^{(-1)^{n-1}}$ is a polynomial and

$$\deg L^*(\bar{g};\ \chi;\ t)^{(-1)^{n-1}} = (\deg \bar{g})^n.$$

We note that the statement is true when $n=1$ by Eqn. (30) of [2], and is true (for any n) when $\deg \bar{g} = 1$ by direct calculation. When this statement holds, it allows us to obtain information about the related character sum

$$S_m(\bar{g},\chi) = \sum_{x\in(\boldsymbol{F}_{q^m})^n} \chi(\bar{g}(x)),$$

where the coordinate hyperplanes are not deleted. Put

$$L(\bar{g};\ \chi;\ t) = \exp\left(\sum_{m=1}^{\infty} S_m(\bar{g},\chi)t^m/m\right). \tag{6.4}$$

We follow the procedure of [8] to compute $\deg L(\bar{g};\ \chi;\ t)^{(-1)^{n-1}}$. For any subset A of $\{1,2,\dots,n\}$, let $n(A)$ be the cardinality of A and let $\bar{g}_A$ be the polynomial in $n-n(A)$ variables obtained from $\bar{g}$ by setting $x_i=0$ for $i\in A$. Then $S_m(\bar{g},\chi)=\sum_A S_m^*(\bar{g}_A,\chi)$, consequently

$$L(\bar{g};\ \chi;\ t)^{(-1)^{n-1}} = \prod_A \left(L(\bar{g}_A;\ \chi_A;\ t)^{(-1)^{n-n(A)-1}}\right)^{(-1)^{n(A)}} \tag{6.5}$$

If $\bar{g}$ is regular then so is $\bar{g}_A$ for all A; furthermore, $\deg \bar{g} = \deg \bar{g}_A$. Hence

$$\deg L(\bar{g}; \chi; t)^{(-1)^{n-1}} = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (\deg \bar{g})^{n-k}$$

$$= ((\deg \bar{g}) - 1)^n.$$

In the case $n = 1$, it is known that if the $\bar{g}_i$ are distinct and irreducible, then

$$\deg L(\bar{g}_1, \ldots, \bar{g}_b; \chi_1, \ldots, \chi_b; t) = \left(\sum_{i=1}^{b} \deg \bar{g} \right) - 1.$$

This can be derived from results in [11]. A direct proof was given by Davenport [6].

7. Total degree of the L-function

We follow closely the method of [5], which involves evaluating the sums in Theorem 3. While we can explicitly compute the x-coordinates, we can only give a lower bound for the y-coordinates. This will be sufficient to estimate the total number of zeros and poles of the L-function.

Recall the basic facts about the binomial coefficients $c(s) = \binom{s+n-1}{n-1}$:

$$\sum_{s=0}^{\infty} c(s) z^s = (1-z)^{-n}, \tag{7.1}$$

hence $\sum_{s=0}^{r} c(s)$ is the coefficient of z^r in $(1-z)^{-n}(1-z)^{-1}$:

$$\sum_{s=0}^{r} c(s) = \binom{r+n}{n}. \tag{7.2}$$

One has from (7.1)

$$\sum_{s=0}^{\infty} s c(s) z^{s-1} = n(1-z)^{-n-1}, \tag{7.3}$$

hence $\sum_{s=0}^{r} s c(s)$ is the coefficient of z^{r-1} in $n(1-z)^{-n-1}(1-z)^{-1}$:

$$\sum_{s=0}^{r} s c(s) = n \binom{r+n}{n+1}$$

$$= \frac{nr}{n+1} \binom{r+n}{n}. \tag{7.4}$$

Assume for the moment that $\nu > 0$. By Proposition 2 and (7.2),

$$W(0)+\sum_{r=0}^{N} W\left(r+\frac{\nu}{p-1}\right)=\sum_{s=0}^{(N+1)D+R} c(s)$$

$$=\binom{(N+1)D+R+n}{n}.$$

Using (7.4) we have

$$\sum_{r=0}^{N}\left(r+\frac{\nu}{p-1}\right)W\left(r+\frac{\nu}{p-1}\right)=\sum_{r=0}^{N}\left(r+\frac{\nu}{p-1}\right)\sum_{s=rD+R+1}^{(r+1)D+R} c(s)$$

$$\geqslant \sum_{r=0}^{N}\sum_{s=rD+R+1}^{(r+1)D+R}\left(\frac{s-R-D}{D}+\frac{\nu}{p-1}\right)c(s)$$

$$=\frac{1}{D}\sum_{s=R+1}^{(N+1)D+R} sc(s)-\left(R+D-\frac{D\nu}{p-1}\right)c(s)$$

$$=\frac{1}{D}\left[\frac{n((N+1)D+R)}{n+1}\binom{(N+1)D+R+n}{n}-\frac{nR}{n+1}\binom{R+n}{n}\right]$$

$$-\frac{1}{D}\left(R+D-\frac{D\nu}{p-1}\right)\left[\binom{(N+1)D+R+n}{n}-\binom{R+n}{n}\right]$$

$$=\frac{1}{D}\left[\frac{nND-R-D+\dfrac{D(n+1)\nu}{p-1}}{n+1}\binom{(N+1)D+R+n}{n}\right.$$

$$\left.+\frac{nD+D+R-\dfrac{D(n+1)\nu}{p-1}}{n+1}\binom{R+n}{n}\right].$$

We have proved

Proposition 4: *Under the hypotheses of Theorem* 3, *if* $\nu > 0$, *then the Newton polygon of* $\det(I-t\alpha_H)$ *is contained in the convex closure of the* *points* $(0, 0)$, $(\binom{R+n}{n}, 0)$, *and*

$$\left(\binom{(N+1)D+R+n}{n}, \frac{p-1}{Dp}\left[\frac{nND-R-D+\dfrac{D(n+1)\nu}{p-1}}{n+1}\right.\right.$$

$$\left.\left.\times\binom{(N+1)D+R+n}{n}+\frac{nD+D+R-\dfrac{D(n+1)\nu}{p-1}}{n+1}\binom{R+n}{n}\right]\right), \tag{7.5}$$

$N = 0, 1, 2, \ldots$. (*The same argument shows that if* $\nu = 0$, *then the same statement holds provided the point* $(\binom{R+n}{n}, 0)$ *is deleted.*)

Write as in (6.1)

$$L^*(\bar{g}_1, \ldots, \bar{g}_b; \chi_1, \ldots, \chi_b; t)^{(-1)^{n-1}} = \prod_{i=1}^{r}(1-\rho_i t)\Big/\prod_{j=1}^{s}(1-\eta_j t).$$

By [7, Exp. XXI, Cor. 5.5.3(iii)], $0 \leqslant \operatorname{ord}_q \rho_i, \operatorname{ord}_q \eta_j \leqslant n$. Writing out the right-hand side of (2.17),

$$\frac{\Pi(1-\rho_i t)}{\Pi(1-\eta_j t)} = \prod_{m=0}^{n} \det(I - q^m t\alpha_H)^{(-1)^m\binom{n}{m}}.$$

Hence the zeros and poles of $L^*(t)$ all occur among the zeros of $\Pi_{m=0}^{n} \det(I - q^m t\alpha_H)^{\binom{n}{m}}$ of $\operatorname{ord}_q \leqslant n$. Let N_m be the number of zeros of $\det(I - q^m t\alpha_H)$ of $\operatorname{ord}_q \leqslant n$. Then

$$\text{tot.deg}\, L^*(t) \leqslant \sum_{m=0}^{n} \binom{n}{m} N_m. \tag{7.6}$$

Now N_m is the total length of the projections on the x-axis of the sides of slope $\leqslant n - m$ of the Newton polygon of $\det(I - t\alpha_H)$, hence N_m can be estimated by Proposition 4. Let $\epsilon(n)$ be the least integer $\geqslant ((n+1)p - \nu)/(p-1)$. Then it is easily checked that the slope of the line through $(0, 0)$ and the point given by (7.5) with $N = \epsilon(n) + 2 - m$ has slope $\geqslant n - m$, hence N_m is bounded by the x-coordinate of this point:

$$N_m \leqslant \binom{(\epsilon(n)+3-m)D+R+n}{n}.$$

From (7.6) and the fact that $R < D$,

$$\operatorname{tot.deg} L^*(t) \leqslant \sum_{m=0}^{n} \binom{n}{m} \binom{(\epsilon(n)+4-m)D+n}{n}. \tag{7.7}$$

Let C denote the right-hand side of (7.7). It is the coefficient of $x^{(\epsilon(n)+4)D}$ in $(1+x^D)^n(1-x)^{-n-1}$, hence is the residue at 0 of the differential

$$x^{-(\epsilon(n)+4-n)D}(1+x^{-D})^n(1-x)^{-n}\frac{\mathrm{d}x}{x(1-x)}.$$

Making the substitution $x \mapsto z/(1+z)$ and using the invariance of residues, $C = \operatorname{res}_0 F(z)\mathrm{d}z/z$, where

$$F(z) = \left(1+\frac{1}{z}\right)^{(\epsilon(n)+4-n)D}\left(1+\left(1+\frac{1}{z}\right)^{D}\right)^{n}(1+z)^n.$$

Since the coefficients in the Laurent expansion of $F(z)$ are all non-negative, this residue is bounded by $F(z)$ for all $z > 0$. For example, we may take $z = D$. Using $(1+1/D)^D < \mathrm{e}$ we get

$$C \leqslant \mathrm{e}^{\epsilon(n)+4-n}(1+\mathrm{e})^n(D+1)^n. \tag{7.8}$$

THEOREM 6: *Under the hypotheses of Theorem* 3,

$$\operatorname{tot.deg} L^*(\bar{g}_1,\dots,\bar{g}_b;\ \chi_1,\dots,\chi_b;\ t)$$
$$\leqslant \exp[5+(n+p-2)/(p-1)](\mathrm{e}+1)^n(D+1)^n.$$

PROOF: It is easily checked that $\epsilon(n)+4-n \leqslant 5+[(n+p-2)/(p-1)]$. One then uses (7.8). QED

We can still estimate the total degree, even without the hypotheses of Theorem 3. If the characters $\chi_1,\dots,\chi_b$ take values in the unramified extension of $\boldsymbol{Q}_p$ of degree a, the estimate in Theorem 2 is modified as follows: $C(\mu, k_0, k;\ \mu', k_0', k')$ is the coefficient of $R_{\mu'}x_0^{k_0'}\tilde{h}^{k'}$ in $\alpha_H(R_\mu x_0^{k_0}\tilde{h}^k)$, then

$$\operatorname{ord} C\left(\mu, k_0, k;\ \mu', k_0', k'\right) \geqslant \max\left\{0,\ -k'-\lambda\left(k+\min_{\iota}\{\mu_\iota\}\right)\right\}. \tag{7.9}$$

It follows that the polygon described in Theorem 3 is a lower bound for the Newton polygon of $\det(I - t\alpha_H)$ computed with respect to "ord" (rather than "ord_q"). Consequently, to obtain a lower bound for the Newton polygon of $\det(I - t\alpha_H)$ with respect to "ord_q" simple divide each y-coordinate by a. Put $\mu = \min_i\{\mu_i\}$, $R = [\Sigma e_i \mu_i/(p^a - 1)]$.

Proposition 5: *If* $\mu > 0$ *the Newton polygon of* $\det(I - t\alpha_H)$ *with respect to "*ord_q*" is contained in the convex closure of the points* $(0, 0)$, $(\binom{R+n}{n}, 0)$, *and*

$$\left(\binom{(N+1)D+R+n}{n}, \frac{p-1}{aDp}\left[\frac{nND - R - D + \dfrac{D(n+1)\mu}{p-1}}{n+1}\right.\right.$$

$$\left.\left.\times\binom{(N+1)D+R+n}{n} + \frac{nD + D + R - \dfrac{D(n+1)\mu}{p-1}}{n+1}\binom{R+n}{n}\right]\right),$$

$N = 0, 1, 2, \ldots$. *If* $\mu = 0$, *the same statement holds when the point* $(\binom{R+n}{n}, 0)$ *is deleted.*

Applying the argument of Theorem 6 to this estimate for the Newton polygon gives

Theorem 7:

$$\text{tot.deg}\, L^*(\bar{g}_1,\ldots,\bar{g}_b;\, \chi_1,\ldots,\chi_b;\, t)$$
$$\leqslant \exp[5 + (n+p-2)/(p-1)](e+1)^n(aD+1)^n.$$

8. Unit root

We investigate circumstances under which $L^*(\bar{g}_1,\ldots,\bar{g}_b;\, \chi_1,\ldots,\chi_b;\, t)$ has a unique unit root. By (2.17), we see that this happens if and only if $\det(I - t\alpha_H)$ has a unique unit root, in which case these unit roots are equal. By Proposition 5, if $\mu > 0$ then $\det(I - t\alpha_H)$ will have at most one unit root when $\binom{R+n}{n} = 1$, i.e., when $R = 0$.

Theorem 8: *If* $R = 0$, $\prod_{i=1}^b \bar{g}_i(0,\ldots,0) \neq 0$, *and* $\mu > 0$ *(i.e., all* χ_i *are non-trivial), then* $L^*(\bar{g}_1,\ldots,\bar{g}_b;\, \chi_1,\ldots,\chi_b;\, t)$ *has a unique unit root.*

Proof: By the above remarks, it suffices to show there is at least one unit root. By (2.17), this will be the case provided $\text{Tr}\,\alpha_H$ is a unit. In the notation of the paragraph preceding Proposition 5, we must show that

$\Sigma C(\mu, k_0, k; \mu, k_0, k)$ is a unit, where the sum is over all $R_\mu x_0^{k_0}\tilde{h}^k$ with

$$\deg R_\mu x_0^{k_0}\tilde{h}^k = 0 \quad \text{and} \quad k_0 \geqslant -R = 0. \tag{8.1}$$

Estimate (7.9), together with our hypothesis on the μ_i's, implies that for $k \leqslant -1$,

$$\operatorname{ord} C(\mu, k_0, k; \mu, k_0, k) \geqslant 1.$$

For $k = 0$, there is only one basis element satisfying (8.1), namely, $R_\mu x_0^{k_0}\tilde{h}^k = 1$ (i.e., $k = k_0 = 0$, $R_\mu = 1$). Thus we are reduced to showing that the coefficient of 1 in the expansion of $\alpha_H(1)$ in terms of the orthonormal basis is a unit.

Now $\alpha_H(1) = \psi_q(\prod_{i=1}^{c} H_i(x)^{\mu_i})$, where the H_i are given by (2.10). The assumption $\prod_{i=1}^{b}\bar{g}_i(0,\ldots,0) \neq 0$ implies that each homogenization $\hat{g}_i$ contains a term of the form $\gamma_i x_0^{d_i}$, where $d_i = \deg \bar{g}_i$ and γ_i is a non-zero constant. Hence the $\bar{h}_j$'s, which are the irreducible factors of the $\hat{g}_i$'s, all contain a term of the form $\gamma'_j x_0^{e_j}$, where $e_j = \deg \bar{h}_j$ and γ'_j is a non-zero constant. It follows that the coefficient of $x_0^{e_j}$ in h_j is a root of unity. Therefore

$$\prod_{i=1}^{c} H_i(x)^{\mu_i} = \frac{\prod_{i=1}^{c} h_i^{\mu_i}}{x_0^{\Sigma e_i \mu_i}} \sum_{r=0}^{\infty} a'_r B'_r(x)\tilde{h}(x)^{-rp}, \tag{8.2}$$

where as in the proof of Theorem 2 $a'_r \in \mathcal{O}_a$ satisfies $a'_0 = 1$ and $\operatorname{ord} a'_r \geqslant r$, $B'_r(x) \in \mathcal{O}_a[x]$ satisfies $B'_0(x) = 1$ and $\deg B'_r(x) = Drp$. Since we are doing a mod p calculation, we may, by [3, Lemma 1], ignore the terms with $r \geqslant 1$. Our above remarks show that the coefficient of $x_0^{\Sigma e_i \mu_i}$ in $\prod h_i^{\mu_i}$ is a root of unity. The assertion now follows from (8.2). QED

REMARK: We believe that under the hypotheses of Theorem 8, the unit root is $\prod_{i=1}^{b}\chi_i(\bar{g}_i(0,\ldots,0))$.

EXAMPLE: Assume $p \neq 2$. Let $g(x) \in \boldsymbol{F}_p[x]$ be a quadratic polynomial in one variable, say,

$$g(x) = ax^2 + bx + c, \quad a \neq 0, \quad a, b, c \in \boldsymbol{F}_p.$$

Assume that $3|(p-1)$ and let χ_1, χ_2 be the cubic characters, say,

$$\chi_1 = \omega^{(p-1)/3}, \quad \chi_2 = \omega^{2(p-1)/3},$$

where ω is the Teichmüller character on $\boldsymbol{F}_p^\times$. Suppose that $b^2 - 4ac \neq 0$.

Then the projective completion $\tilde{C}$ of the curve $y^3 = ax^2 + bx + c$ is non-singular, hence is an elliptic curve. Its zeta function is therefore of the form

$$Z(\tilde{C}, t) = \frac{(1 - \pi_1 t)(1 - \pi_2 t)}{(1 - t)(1 - pt)}.$$

Since there is exactly one point at infinity on $\tilde{C}$, the number N_m of solutions of $y^3 = ax^2 + bx + c$ with $x, y \in \boldsymbol{F}_{p^m}$ is

$$N_m = p^m - \pi_1^m - \pi_2^m.$$

We can also count the number of solutions using the cubic characters: denoting by $\chi_i^{(m)}$ the composition of χ_i with the norm map from $\boldsymbol{F}_{p^m}$ to $\boldsymbol{F}_p$,

$$1 + \chi_1^{(m)}(g(x)) + \chi_2^{(m)}(g(x)) = \begin{cases} 3 & \text{if} \quad g(x) \in \left(\boldsymbol{F}_{p^m}^\times\right)^3 \\ 1 & \text{if} \quad g(x) = 0 \\ 0 & \text{if} \quad g(x) \notin \left(\boldsymbol{F}_{p^m}^\times\right)^3. \end{cases}$$

Hence

$$N_m = p^m + \sum_{x \in \boldsymbol{F}_{p^m}} \chi_1^{(m)}(g(x)) + \sum_{x \in \boldsymbol{F}_{p^m}} \chi_2^{(m)}(g(x)).$$

The L-functions associated to (g, χ_1) and (g, χ_2) are linear polynomials (for example, by [2, Lemma 1 and Eqn. (21)]), hence $\sum_{x \in \boldsymbol{F}_{p^m}} \chi_1^{(m)}(g(x))$ equals either $-\pi_1^m$ or $-\pi_2^m$ and $\sum_{x \in \boldsymbol{F}_{p^m}} \chi_2^{(m)}(g(x))$ equals the other.

We can determine which is which if $c \neq 0$. Since $p \equiv 1 (\text{mod } 3)$, $\tilde{C}$ is not supersingular so exactly one of π_1 and π_2 is a p-adic unit, say π_1. Since $c \neq 0$, Theorem 8 applies to (g, χ_1) and we conclude that the L-function associated to the sum $\sum_{x \in \boldsymbol{F}_p^\times m} \chi_1^{(m)}(g(x))$ has a unique unit root. But

$$\sum_{x \in \boldsymbol{F}_{p^m}^\times} \chi_1^{(m)}(g(x)) = \left(\sum_{x \in \boldsymbol{F}_{p^m}^\times} \chi_1^{(m)}(g(x)) \right) - \chi_1(g(0)),$$

and the right-hand side is either $-\pi_1^m - \chi_1(g(0))^m$ or $-\pi_2^m - \chi_1(g(0))^m$. Since $\chi(g(0))$ is a root of unity (hence a unit) and since $\sum_{x \in \boldsymbol{F}_p^\times m} \chi_1^{(m)}(g(x))$ has a unique unit root, we conclude

$$\sum_{x \in \boldsymbol{F}_{p^m}} \chi_1^{(m)}(g(x)) = -\pi_2^m.$$

Note also that the sum$\sum_{x\in \boldsymbol{F}_{p^m}^{\times}}\chi_2^{(m)}(g(x)) = -\pi_1^m - \chi_2(g(0))^m$ has 2 unit roots, so that the hypothesis $R > 0$ of Theorem 8 is indeed necessary.

References

[1] A. ADOLPHSON: An index theorem for p-adic differential operators. *Trans. Amer. Math. Soc. 216* (1976) 279–293.

[2] A. ADOLPHSON: Appendix to: B. Dwork, Lectures on p-adic differential equations, Grundlehren der mathematischen Wissenschaften 253. New York, Heidelberg, Berlin: Springer-Verlag (1982).

[3] A. ADOLPHSON and S. SPERBER: Exponential sums on the complement of a hypersurface. *Amer. J. Math. 102* (1980) 461–487.

[4] E. BOMBIERI: On exponential sums in finite fields. *Amer. J. Math. 88* (1966) 71–105.

[5] E. BOMBIERI: On exponential sums in finite fields, II. *Inventiones Math. 47* (1978) 29–39.

[6] H. DAVENPORT: On character sums in finite fields. *Acta Math. 71* (1939) 99–121.

[7] P. DELIGNE and N. KATZ: Groupes de Monodromie en Géométrie Algébrique, *Lecture Notes in Math. No. 340.* Berlin, Heidelberg, New York: Springer-Verlag (1973).

[8] B. DWORK: On the rationality of the zeta function of an algebraic variety. *Amer. J. Math. 82* (1960) 631–648.

[9] B. DWORK: On the zeta function of a hypersurface. *Publ. Math. I.H.E.S. 12* (1962) 5–68.

[10] B. DWORK: On the zeta function of a hypersurface, II. *Ann. Math. 80* (1964) 227–299.

[10] (a) B. DWORK: Lectures on p-adic differential equations, Grundlehren der Mathematischen Wissenschaften 253. New York, Heidelberg, Berlin: Springer-Verlag (1982).

[11] H. HASSE: Theorie der relativ-zyklischen algebraischen Funktionenkörper, inbesondere bei endlichem Konstantenkörper. *J. Reine u. Angew. math.* 172 (1934) 37–54.

[12] L. ILLUSIE: Théorie de Brauer et caractéristique d'Euler-Poincaré. *Astérisque 82–83* (1981) 161–172.

[13] D. REICH: A p-adic fixed point formula. *Amer. J. Math. 91* (1969) 835–850.

[14] J-P. SERRE: Endomorphismes completement continus des espaces de Banach p-adiques. *Publ. Math. I.H.E.S. 12* (1962) 69–85.

(Oblatum 18-VIII-1982 & 26-V-1983)

A. Adolphson
Department of Mathematics
Oklahoma State University
Stillwater, OK 74078
USA

Steven Sperber
School of Mathematics
University of Minnesota
Minneapolis, MN 55455
USA