PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 123, Number 1, January 1995

A CHEVALLEY-WARNING APPROACH TO p-ADIC ESTIMATES OF CHARACTER SUMS

DAQING WAN

(Communicated by William Adams)

ABSTRACT. The elementary Chevalley-Warning congruence method is applied to obtain several p-adic estimates of character sums over finite fields.

1. INTRODUCTION

Let $\mathbf{F}_q$ be the finite field of q elements with characteristic p. Let $F_i(x_1, \ldots, x_n)$ $(i = 1, \ldots, r)$ be polynomials of degree d_i over $\mathbf{F}_q$. The classical Chevalley-Warning theorem asserts that if $n > \sum_i d_i$, then the characteristic p divides the number $N_q(F_1, \ldots, F_r)$ of $\mathbf{F}_q$-rational solutions of the system

$$F_1(x_1, \ldots, x_n) = F_2(x_1, \ldots, x_n) = \cdots = F_r(x_1, \ldots, x_n) = 0. \tag{1.1}$$

The proof of this theorem is very simple and elegant; see [8]. It is based on the following congruence formula:

$$N_q(F_1, \ldots, F_r) \equiv \sum_{x \in \mathbf{F}_q^n} (1 - F_1(x)^{q-1}) \cdots (1 - F_r(x)^{q-1}) \pmod{p}, \tag{1.2}$$

a principal first noted by Lebesgue in 1837 (see the notes of Chapter 7 in [5]).

The Chevalley-Warning theorem was greatly improved by Ax [3] (for the case $r = 1$) and Katz [4] (for general r). The Ax-Katz theorem asserts that if b is the least integer such that

$$b \geq \frac{n - \sum_i d_i}{\max_i d_i}, \tag{1.3}$$

then q^b divides $N_q(F_1, \ldots, F_r)$. Ax [3] also obtained a weaker result for general r, which replaces the right side of (1.3) by $(n - \sum_i d_i)/\sum_i d_i$. The Ax-Katz theorem is best possible in the sense that for each n and each multiple degree $(d_1, \ldots, d_r)$, there are polynomials F_i of degree d_i such that the highest power of q dividing $N_q(F_1, \ldots, F_r)$ is exactly q^b. Instead of using a congruence formula similar to (1.2), Ax used the well-known expression of the number $N_q(F_1, \ldots, F_r)$ in terms of exponential sums. Ax's proof is p-adic in nature and uses the Stickelberger theorem on Gauss sums. Even though there

Received by the editors April 14, 1992 and, in revised form, April 16, 1993.
1991 *Mathematics Subject Classification.* Primary 11A07, 11D72, 11T23.

is a quick proof of the Chevalley-Warning theorem, Ax [3] said "there does not seem to be any simple proof of the fact that q divides $N_q(F)$ if $n > d$".

Katz's proof (for general r) is much deeper and uses Dwork's theory of completely continuous operators in an infinite-dimensional p-adic Banach space. The Ax-Katz theorem was generalized to exponential sums by Sperber [9] and Adolphson-Sperber [1, 2]. Their proof is similar to Katz's proof and uses Dwork's p-adic theory. In [10], it was shown that the Katz theorem can be proved by using Ax's method. Aldophson-Sperber [2] then realized that their theorem on exponential sums can also be proved by using Ax's method.

Recently, motivated by coding theoretic considerations, Moreno-Moreno [6, 7] obtained a new theorem which improves the Ax-Katz theorem in certain special cases. Their idea is to reduce the question under consideration from $\mathbf{F}_q$ to the prime field $\mathbf{F}_p$. Also motivated by coding theoretic considerations, Ward [11] recently found a new proof of the Ax theorem (the case $r = 1$). In comparison to Ax's proof, Ward's proof is closer in line to Chevalley-Warning's proof. Essentially, Ward starts with the case $r = 1$ of the limiting congruence formula

$$N_q(F_1, \ldots, F_r) = \sum_{x \in T_q^n} \left(1 - \left(\lim_{k\to\infty} F_1(x)^{q^k}\right)^{q-1}\right) \cdots \left(1 - \left(\lim_{k\to\infty} F_r(x)^{q^k}\right)^{q-1}\right),$$

where T_q is the Teichmüller lifting of $\mathbf{F}_q$ and $F(x)$ has p-adic coefficients. Note that $\lim_{k\to\infty} a^{q^k}$ is simply the Teichmüller lifting of $a \in \mathbf{F}_q$. Ward's proof uses p-adic lifting and avoids the Stickelberger theorem; however, his proof depends on his polarization theory and is not very simple.

Motivated by Ward's proof, in §2 we give a direct and simple proof of the Ax-Katz theorem in the prime field case. Combining with Moreno-Moreno's reduction, this gives a simple proof of the Moreno-Moreno theorem and answers Ax's questions. Our proof is parallel to the Chevalley-Warning proof and uses only congruence formulas over the rational integers and monomial coefficients. The Stickelberger theorem, p-adic liftings, and polarizations are not involved.

For a general finite field, the same congruence proof works if we replace the rational integers by algebraic integers in number fields or by p-adic integers in p-adic fields. Using the congruence argument, in §3 we generalize the Ax-Katz theorem to multiplicative character sums. Finally, in §4 we extend the result in §3 to mixed character sums, which includes Moreno-Moreno's theorem on exponential sums as a special case.

2. The Ax-Katz theorem in prime field case

In this section, we give a direct and simple proof of the Ax-Katz theorem in the prime field case. Let $F_i(x_1, \ldots, x_n)$ $(1 \le i \le r)$ be polynomials of degree d_i with integral coefficients. We are interested in the number $N_q(F_1, \ldots, F_r)$ of solutions of the congruence system

$$(2.1)\quad F_1(x_1, \ldots, x_n) \equiv F_2(x_1, \ldots, x_n) \equiv \cdots \equiv F_1(x_1, \ldots, x_n) \equiv 0 \pmod{p}.$$

Let b be the least integer satisfying (1.3); we need to prove that p^b divides $N_p(F_1, \ldots, F_r)$.

Let S be the set consisting of zero and the g^{ip^n} $(0 \le i \le p-2)$, where g is a fixed primitive root modulo p^n if $p > 2$ and $g = 1$ if $p = 2$. Then S is a complete residue system modulo p. Similar to (1.2), we have the following well-known congruence formula:

$$(2.2)\quad N_p(F_1, \dots, F_r) \equiv \sum_{x \in S^n} (1 - F_1(x)^{(p-1)p^n}) \cdots (1 - F_r(x)^{(p-1)p^n}) \pmod{p^n}.$$

Expanding (2.2) and by induction on r, we see that it suffices to prove that

$$(2.3)\qquad A = \sum_{x \in S^n} \prod_{i=1}^{r} F_i(x)^{(p-1)p^n} \equiv 0 \pmod{p^b}.$$

Let $F_i(x) = \sum_{j=1}^{m_i} a_{ij} x^{e_{ij}}$, where the e_{ij} are vectors in $\mathbf{Z}_{\ge 0}^n$ whose sums of coordinates are at most d_i. Expanding (2.3) and interchanging the summation, we have

$$(2.4)\quad A = \sum_{\substack{k_{i1}+\cdots+k_{im_i}=(p-1)p^n \\ 1 \le i \le r}} \prod_{i=1}^{r} \binom{(p-1)p^n}{k_{i1}, \dots, k_{im_i}} \left(\prod_{i=1}^{r} \prod_{j=1}^{m_i} a_{ij}^{k_{ij}} \right) \sum_{x \in S^n} x^{\sum_{i,j} k_{ij} e_{ij}}.$$

By the classical formula of Legendre, $\operatorname{ord}_p(k!) = (k - \sigma(k))/(p-1)$, where $\sigma(k)$ denotes the sum of the digits in the base p expansion of k. It follows that the p-order of the monomial coefficient in (2.4) is

$$\frac{1}{p-1} \sum_{i=1}^{r} \left((p-1)p^n - (p-1) - \sum_{j=1}^{m_i} (k_{ij} - \sigma(k_{ij})) \right)$$

$$= \frac{1}{p-1} \sum_{i=1}^{r} \left(\sum_{j=1}^{m_i} \sigma(k_{ij}) - (p-1) \right).$$

By our choice of the complete residue system S, the following is valid:

$$(2.5)\quad \sum_{t \in S} t^k \equiv \begin{cases} (g^{k(p-1)p^n} - 1)/(g^{kp^n} - 1) \equiv 0 \pmod{p^n} \\ \qquad\qquad \text{if } (p-1) \text{ does not divide } k, \\ p \pmod{p^n} \qquad \text{if } k = 0, \\ \sum_{i=0}^{p-2} g^{kip^n} \equiv p - 1 \pmod{p^n} \quad \text{if } (p-1) \text{ divides } k \text{ and } k > 0. \end{cases}$$

Thus, in (2.4) we need only to check those terms for which

$$(2.6)\qquad \sum_{i,j} k_{ij} e_{ij} \equiv 0 \pmod{(p-1)},$$

where the congruence means that each coordinate of the vector is divisible by $p-1$. Assume that s of the coordinates in (2.6) are not numerically zero. By (2.4) and (2.5), we are reduced to proving that (noting that the number $N_p(F_1, \dots, F_r)$ is an integer)

$$(2.7)\qquad \frac{n - \sum_i d_i}{\max_i d_i} \le \frac{1}{p-1} \sum_{i=1}^{r} \left(\sum_{j=1}^{m_i} \sigma(k_{ij}) - (p-1) \right) + (n - s).$$

Since $k \equiv \sigma(k) \pmod{(p-1)}$, we can replace k_{ij} by $\sigma(k_{ij})$ in (2.6):

$$\sum_{i,j} \sigma(k_{ij}) e_{ij} \equiv 0 \pmod{(p-1)}. \tag{2.8}$$

Furthermore, s of the coordinates in (2.8) are not numerically zero. Adding these coordinates and letting $d = \max_i d_i$, we deduce that

$$\begin{aligned} s(p-1) - (p-1)\sum_{i=1}^{r} d_i &\le \sum_{i=1}^{r} d_i \left(\sum_{j=1}^{m_i} \sigma(k_{ij}) - (p-1) \right) \\ &\le d \sum_{i=1}^{r} \left(\sum_{j=1}^{m_i} \sigma(k_{ij}) - (p-1) \right). \end{aligned} \tag{2.9}$$

This inequality implies that

$$\begin{aligned} &\frac{1}{p-1} \sum_{i=1}^{r} \left(\sum_{j=1}^{m_i} \sigma(k_{ij}) - (p-1) \right) + (n-s) \\ &\quad \ge \left(\frac{s - \sum_i d_i}{d} \right) + (n-s) \ge \left(\frac{n - \sum_i d_i}{d} \right). \end{aligned}$$

By (2.7), the Ax-Katz theorem is proved for the prime field $\mathbf{F}_p$.

3. Multiplicative character sums

In this section, we generalize the Ax-Katz theorem to multiplicative character sums. Let K_q be the unique unramified extension of degree f over the p-adic rational number field Q_p. Let T_q be the set consisting of the roots of $t^q = t$ in K_q. Then the reduction of T_q modulo p is the finite field $\mathbf{F}_q$. Let T be the Teichmüller character, i.e., $T(\bar{t}) = t$. This is a primitive multiplicative character on $\mathbf{F}_q$ of order $(q-1)$. Any multiplicative character of $\mathbf{F}_q$ is a power of T. Let $\chi_i(t) = T(t)^{j_i}$ $(1 \le i \le r)$ be multiplicative characters of $\mathbf{F}_q$, where the j_i are integers satisfying $0 \le j_i \le q-1$. By convention, $T^0(a)$ is the character with value 1 for all $a \in \mathbf{F}_q$; while $T^{q-1}(a)$ is the character with value 1 for all $a \in \mathbf{F}_q^*$ and $T^{q-1}(0) = 0$. Let $F_i(x_1, \ldots, x_n)$ be polynomials of degree d_i over $\mathbf{F}_q$. Define a character sum by

$$S_q(\chi, F) = \sum_{x \in \mathbf{F}_q^n} \chi_1(F_1(x)) \cdots \chi_r(F_r(x)). \tag{3.1}$$

For an integer $k \ge 0$, define $\sigma_q(k)$ to be the sum of the digits in the expansion of k as a base q number. If $q = p$, then $\sigma_q(k) = \sigma(k)$. For a real number x, define $(x)^*$ to be the smallest integer not less than x. We have the following theorem.

Theorem 3.1. *Let $d = \max_i d_i$ and $q = p^f$. Then the q-order of $S_q(\chi, F)$ is at least*

$$\frac{1}{f} \sum_{a=0}^{f-1} \left(\frac{n - \frac{1}{q-1} \sum_{i=1}^{r} \sigma_q(p^a j_i) d_i}{d} \right)^*. \tag{3.2}$$

Proof. To simplify notation, suppose that the $F_i(x)$ are already lifted to K_q. Since $T(\overline{x}) \equiv x^{q^n} \pmod{q^n}$ for all integral $x \in K_q$, similar to (1.2), we have the following congruence formula:

$$S_q(\chi, F) \equiv \sum_{x \in T_q^n} F_1(x)^{j_1 q^n} \cdots F_r(x)^{j_r q^n} \pmod{q^n}. \tag{3.3}$$

Let $F_i(x) = \sum_{j=1}^{m_i} a_{ij} x^{e_{ij}}$, where the e_{ij} are vectors in $\mathbf{Z}_{\geq 0}^n$ whose sums of coordinates are at most d_i and the a_{ij} are p-adic integers in K_q. Expanding (3.3) and interchanging the summation, we have the following congruence modulo q^n:

(3.4)

$$S_q(\chi, F) \equiv \sum_{\substack{k_{i1}+\cdots+k_{im_i}=j_i q^n \\ 1 \leq i \leq r}} \prod_{i=1}^{r} \binom{j_i q^n}{k_{i1}, \ldots, k_{im_i}} \left(\prod_{i=1}^{r} \sum_{j=1}^{m_i} a_{ij}^{k_{ij}} \right) \sum_{x \in T_q^n} x^{\sum_{i,j} k_{ij} e_{ij}}.$$

By the classical formula of Legendre, $\operatorname{ord}_p(k!) = (k - \sigma(k))/(p-1)$. It follows that the q-order of the monomial coefficient in (3.4) is

$$\begin{aligned} &\frac{1}{f(p-1)} \sum_{i=1}^{r} \left(j_i q^n - \sigma(j_i) - \sum_{j=1}^{m_i} (k_{ij} - \sigma(k_{ij})) \right) \\ &\quad = \frac{1}{f(p-1)} \sum_{i=1}^{r} \left(\sum_{j=1}^{m_i} \sigma(k_{ij}) - \sigma(j_i) \right). \end{aligned} \tag{3.5}$$

By the definition of T_q, the following is valid:

$$\sum_{t \in T_q} t^k = \begin{cases} 0 & \text{if } (q-1) \text{ does not divide } k, \\ q & \text{if } k = 0, \\ q-1 & \text{if } (q-1) \text{ divides } k \text{ and } k > 0. \end{cases} \tag{3.6}$$

Thus, in (3.4) we need only to check those terms for which

$$\sum_{i,j} k_{ij} e_{ij} \equiv 0 \pmod{(q-1)}, \tag{3.7}$$

where the congruence means that each coordinate of the vector is divisible by $p-1$. Since $k \equiv \sigma_q(k) \pmod{(q-1)}$, by (3.7) we have

$$\sum_{i,j} \sigma_q(k_{ij}) e_{ij} \equiv 0 \pmod{(q-1)}. \tag{3.8}$$

Assume that s of the coordinates in (3.7) are not numerically zero. The definition of $\sigma_q(k)$ shows that s of the coordinates in (3.8) are not numerically zero. Adding these coordinates and letting $d = \max_i d_i$, we deduce that

$$\begin{aligned} s(q-1) - \sum_{i=1}^{r} j_i d_i &\leq \sum_{i=1}^{r} d_i \left(\sum_{j=1}^{m_i} \sigma_q(k_{ij}) - j_i \right) \\ &\leq d \sum_{i=1}^{r} \left(\sum_{j=1}^{m_i} \sigma_q(k_{ij}) - j_i \right). \end{aligned} \tag{3.9}$$

Since $\sum_j k_{ij} = j_i q^n \geq 0$ and $\sigma_q(j_i) = j_i$ for all i, we deduce that for all i,

$$\sum_j \sigma_q(k_{ij}) - j_i \equiv 0 \pmod{q-1}. \tag{3.10}$$

It then follows from (3.9) and (3.10) that

$$\left(\frac{s - \frac{1}{q-1}\sum_i j_i d_i}{d}\right)^* (q-1) \leq \sum_{i=1}^{r} \left(\sum_{j=1}^{m_i} \sigma_q(k_{ij}) - j_i\right). \tag{3.11}$$

Let a be a nonnegative integer. If we multiply both sides of (3.7) by p^a, then (3.8) and (3.10) remain true with $\sigma_q(k_{ij})$ replaced by $\sigma_q(p^a k_{ij})$ (and j_i replaced by $\sigma_q(p^a j_i)$). Furthermore, s of their coordinates are not numerically zero. Thus, similar to (3.11), we have

$$\left(\frac{s - \frac{1}{q-1}\sum_i \sigma_q(p^a j_i) d_i}{d}\right)^* (q-1) \leq \sum_{i=1}^{r} \left(\sum_{j=1}^{m_i} \sigma_q(p^a k_{ij}) - \sigma_q(p^a j_i)\right). \tag{3.12}$$

Adding equation (2.12) for $a = 0, 1, \ldots, f-1$, we deduce that

$$\sum_{a=0}^{f-1} \left(\frac{s - \frac{1}{q-1}\sum_i \sigma_q(p^a j_i) d_i}{d}\right)^* (q-1) \leq \frac{q-1}{p-1} \sum_{i=1}^{r} \left(\sum_{j=1}^{m_i} \sigma(k_{ij}) - \sigma(j_i)\right), \tag{3.13}$$

where we used the simple fact that for all integers $k \geq 0$,

$$\sum_{a=0}^{f-1} \sigma_q(p^a k) = \sigma(k)\frac{q-1}{p-1}.$$

By (3.5) and (3.6), we conclude that the q-order of each term in (3.4) is at least

$$\min_{0 \leq s \leq n} \left\{ \frac{1}{f} \sum_{a=0}^{f-1} \left(\frac{s - \frac{1}{q-1}\sum_i \sigma_q(p^a j_i) d_i}{d}\right)^* + (n-s) \right\}$$
$$= \frac{1}{f} \sum_{a=0}^{f-1} \left(\frac{n - \frac{1}{q-1}\sum_i \sigma_q(p^a j_i) d_i}{d}\right)^*.$$

The theorem is proved.

If we take the χ_i to be the trivial characters with $j_i = q-1$ for all i, then the identity $p^a(q-1) = (p^a - 1)q + (q - p^a)$ shows that $\sigma_q(p^a j_i) = q-1$ for all $0 \leq a \leq q-1$. In this case, the number in (3.2) is reduced to the integer b in (1.3) and

$$N_q(F_1, \ldots, F_r) = \sum_{x \in \mathbf{F}_q^n} (1 - \chi_1(F_1(x))) \cdots (1 - \chi_r(F_r(x))).$$

Thus, Theorem 3.1 includes the Ax-Katz theorem as a special case. Using the inequality $(x)^* + (y)^* \geq (x+y)^*$ and the identity $\sum_{a=0}^{f-1} \sigma_q(p^a j) = \sigma(j)(q-1)/(p-1)$, we obtain

Corollary 3.2. *The q-order of $S_q(\chi, F)$ is at least*

$$\frac{1}{f}\left(\frac{nf - \frac{1}{p-1}\sum_i \sigma(j_i)d_i}{d}\right)^*. \tag{3.14}$$

4. Mixed character sums

In this section, we prove that similar results are true for mixed character sums. We shall combine the congruence method, Moreno-Moreno's reduction, and Ax's method. An alternative approach (not discussed here) would be to replace the congruence method by Jacobi sums and Stickelberger's theorem. Let $\chi_i = T^{j_i}$ $(1 \le i \le r)$ be multiplicative characters of $\mathbf{F}_q$ as above. Let ψ be a fixed nontrivial additive character of $\mathbf{F}_q$. Let $F_i(x_1, \dots, x_n)$ $(1 \le i \le r+1)$ be polynomials of degree d_i over $\mathbf{F}_q$. Define a mixed character sum by

$$S_q(\chi, \psi, F) = \sum_{x \in \mathbf{F}_q^n} \chi_1(F_1(x)) \cdots \chi_r(F_r(x))\psi(F_{r+1}(x)). \tag{4.1}$$

For $1 \le i \le r+1$, let

$$h_i = \max_{(k_1, \dots, k_n)} \sigma(k_1) + \cdots + \sigma(k_n),$$

where the maximum is taken over the degrees of all monomials $x_1^{k_1} \cdots x_n^{k_n}$ in F_i. We have the following theorem.

Theorem 4.1. *The p-order $S_q(\chi, \psi, F)$ is at least*

$$\frac{f}{\max_{1 \le i \le r+1} h_i}\left(n - \frac{1}{f(p-1)}\sum_{i=1}^{r} \sigma(j_i)h_i\right). \tag{4.2}$$

Proof. We assume that the $F_i(x)$ are already lifted to a polynomial in $K_q[x]$ of degree d_i. Similar to §3, we have the following congruence formula

$$S_q(\chi, \psi, F) \equiv \sum_{x \in T_q^n} F_1(x)^{j_1 q^n} \cdots F_r(x)^{j_r q^n} \psi(F_{r+1}(x)) \pmod{q^n}, \tag{4.3}$$

where for simplicity, $\psi(F_{r+1}(x))$ means the value of ψ at the reduction of $F_{r+1}(x)$ modulo p. We use Moreno-Moreno's reduction to reduce the above sum to a sum over T_p^n. Choose elements $\alpha_1, \dots, \alpha_f$ in T_q such that their reduction is a basis of $\mathbf{F}_q$ over $\mathbf{F}_p$. Then every element x_i of T_q can be uniquely written in the form $x_i \equiv y_{i1}\alpha_1 + \cdots + y_{if}\alpha_f \pmod{p}$, where the y_{ij} are elements in T_p. Let $k = k_0 + k_1 p + k_2 p^2 + \cdots$ be a positive integer. Then

$$\begin{aligned} x_i^k &\equiv \left(\sum_{j=1}^{f} y_{ij}\alpha_j\right)^{k_0 + k_1 p + k_2 p^2 + \cdots} \\ &\equiv \left(\sum_{j=1}^{f} y_{ij}\alpha_j\right)^{k_0} \left(\sum_{j=1}^{f} y_{ij}\alpha_j^p\right)^{k_1} \cdots \pmod{p}. \end{aligned} \tag{4.4}$$

Thus, we can replace the polynomial $F_{r+1}(x)$ of degree d_{r+1} by a p-adic integral polynomial $G_{r+1}(y)$ in $K_q[y_{11}, y_{12}, \dots, y_{nf}]$ of degree at most h_{r+1}, and the

variables y_{ij} take values in T_p. Since the y_{ij} are in T_p, we have $\psi(G_{r+1}(y)) = \psi_p(\mathrm{tr}(G_{r+1}(y))) = \psi_p(G'_{r+1}(y))$, where ψ_p is an additive character ψ_p of $\mathbf{F}_p$ and the polynomial $G'_{r+1}(y)$ has coefficients in $\mathbf{Z}_p$. For each $1 \le i \le r$, let $j_i = j_i(0) + j_i(1)p + \cdots + j_i(f-1)p^{f-1}$ be the base p expansion of j_i. Then the congruence reduction idea as in (4.4) shows that we can replace each polynomial $F_i^{j_i}(x)$ (coming from $\chi_i(F_i) = T(F_i^{j_i})$) by a product polynomial $\Pi_{k=0}^{f-1} G_{ik}^{j_i(k)}(y)$, where each G_{ik} is a p-adic integral polynomial in $K_q[y_{11}, y_{12}, \ldots, y_{nf}]$ of degree at most h_i, and the variables y_{ij} take values in T_p. Thus, we are reduced to the case $f = 1$ except that the polynomials $F_i(x)$ $(1 \le i \le r)$ may have coefficients in the extension K_q. Namely, we are reduced to consider

$$S_p(\chi, \psi, F) \equiv \sum_{x \in T_q^n} F_1(x)^{j_1 p^n} \cdots F_r(x)^{j_r p^n} \psi_p(F_{r+1}(x)) \pmod{p^n}, \tag{4.5}$$

where $0 \le j_i \le p-1$, each polynomial $F_i(x)$ has at most degree d_i with p-adic integral coefficients in the extension K_q, and $F_{r+1}(x)$ has coefficients in $\mathbf{Z}_p$. We need to prove that the p-order of the sum in (4.5) is at least

$$\frac{1}{\max_{1 \le i \le r+1} d_i} \left(n - \frac{1}{(p-1)} \sum_i j_i d_i \right). \tag{4.6}$$

For $1 \le i \le r$, let $F_i(x) = \sum_{j=1}^{m_i} a_{ij} x^{e_{ij}}$, where the e_{ij} are vectors in $\mathbf{Z}_{\ge 0}^n$ whose sums of coordinates are at most d_i. Let $F_{r+1}(x) = \sum_{j=1}^{m} b_j x^{e_j}$, where the e_j are vectors in $\mathbf{Z}_{\ge 0}^n$ whose sums of coordinates are at most d_{r+1}. The multiplicative part can be expanded as before:

$$\prod_{i=1}^{r} F_i(x)^{j_i p^n} = \sum_{\substack{k_{i1} + \cdots + k_{im_i} = j_i p^n \\ 1 \le i \le r}} \prod_{i=1}^{r} \binom{j_i p^n}{k_{i1}, \ldots, k_{im_i}} \left(\prod_{i=1}^{r} \prod_{j=1}^{m_i} a_{ij}^{k_{ij}} \right) x^{\sum_{i,j} k_{ij} e_{ij}}. \tag{4.7}$$

The p-order of the monomial coefficient in (4.7) is computed to be

$$\frac{1}{p-1} \sum_{i=1}^{r} \left(j_i p^n - j_i - \sum_{j=1}^{m_i} (k_{ij} - \sigma(k_{ij})) \right) = \frac{1}{p-1} \sum_i \left(\sum_j \sigma(k_{ij}) - j_i \right). \tag{4.8}$$

For the additive part, we use Gauss sums and Stickelberger's theorem. For integer k with $0 \le k \le p-2$, define the Gauss sum

$$g_k = \sum_{x \in T_p} t^{p-1-k} \psi_p(x).$$

Let $\sum_k G(k) t^k$ be a polynomial of degree $p-1$ such that

$$\psi_p(\bar{t}) = \sum_{k=0}^{p-1} G(k) t^k, \tag{4.9}$$

for all $t \in T_p$. One checks that $G(0) = 1$, $G(p-1) = -p/(p-1)$ and for $1 \le k \le p-2$, $G(k) = g_k/(p-1)$. The Stickelberger theorem asserts that the p-order of g_k is $k/(p-1)$ (this prime field case can be proved easily). Thus, the p-order of $G(k)$ is $k/(p-1)$ for all $0 \le k \le p-1$. For simplicity,

we define $\psi_p(x) = \psi_p(\bar{x})$ if x is a p-adic integer in $\mathbf{Z}_p$. Using (4.9), for all $x \in T_p^n$ we have the expansion

$$\begin{aligned}\psi_p(F_{r+1}(x)) &= \prod_{j=1}^{m} \psi_p(b_j x^{e_j}) \\ &= \sum_{l_1,\dots,l_m=0}^{p-1} \left(\prod_{j=1}^{m} G(l_j)\right) \prod_{j=1}^{m} (b_j x^{e_j})^{l_j}.\end{aligned} \tag{4.10}$$

The p-order of the coefficient in (4.10) is $(\sum_{j=1}^{m} l_j)/(p-1)$.

Substituting (4.7) and (4.10) into (4.5), multiplying them out, and using the definition of T_q, we need only to check those terms for which

$$\sum_{i=1}^{r}\sum_{j=1}^{m_i} k_{ij}e_{ij} + \sum_{j=1}^{m} l_j e_j \equiv 0 \pmod{(p-1)}, \tag{4.11}$$

where the congruence means that each coordinate of the vector is divisible by $(p-1)$. Assume that s of the coordinates in (4.11) are not numerically zero, and let $d = \max_{1\le i\le r+1} d_i$. By the above computation, we are reduced to proving that

(4.12)

$$\frac{1}{d}\left(n - \frac{1}{p-1}\sum_{i=1}^{r} j_i d_i\right) \le \frac{1}{p-1}\left(\sum_{i=1}^{r}\left(\sum_{j=1}^{m_i}\sigma(k_{ij}) - j_i\right) + \sum_{j=1}^{m} l_j\right) + (n-s).$$

Replacing k_{ij} by $\sigma(k_{ij})$ in (4.11), we get

$$\sum_{i=1}^{r}\sum_{j=1}^{m_i} \sigma(k_{ij})e_{ij} + \sum_{j=1}^{m} l_j e_j \equiv 0 \pmod{(p-1)}. \tag{4.13}$$

Furthermore, s of the coordinates in (4.13) are not numerically zero. Adding these coordinates, we deduce that

$$\begin{aligned}s(p-1) - \sum_{i=1}^{r} j_i d_i &\le \sum_{i=1}^{r} d_i \left(\sum_{j=1}^{m_i}\sigma(k_{ij}) - j_i\right) + \sum_{j=1}^{m} l_j d_{r+1} \\ &\le d\left(\sum_{i=1}^{r}\left(\sum_{j=1}^{m_i}\sigma(k_{ij}) - j_i\right) + \sum_{j=1}^{m} l_j\right).\end{aligned} \tag{4.14}$$

By (4.12), the p-order of $S_p(\chi, \psi, F)$ is at least

$$\begin{aligned}&\frac{1}{p-1}\left(\sum_{i=1}^{r}\left(\sum_{j=1}^{m_i}\sigma(k_{ij}) - j_i\right) + \sum_{j=1}^{m} l_j\right) + (n-s) \\ &\quad\ge \left(\frac{s - \frac{1}{p-1}\sum_{i=1}^{r} j_i d_i}{d}\right) + (n-s) \ge \frac{1}{d}\left(n - \frac{1}{p-1}\sum_{i=1}^{r} j_i d_i\right).\end{aligned}$$

Theorem 4.1 is proved.

If we take the χ_i to be the characters with $j_i = 0$ and take F_i with $d_i = 1$ for all $i \leq r$, then

$$S_q(\chi, \psi, F) = S_q(\psi, F_{r+1}) = \sum_{x \in \mathbf{F}_q^n} \psi(F_{r+1}(x)) \tag{4.15}$$

is the exponential sum treated by Sperber [9]. Theorem 4.1 shows that the p-order of the exponential sum in (4.15) is at least fn/h_{r+1}. This is a theorem of Moreno-Moreno [6] on exponential sums, which improves a theorem of Sperber [9].

Corollary 4.2. *The q-order of $S_q(\chi, \psi, F)$ is at least*

$$\frac{1}{\max_{1 \leq i \leq r+1} d_i} \left(n - \frac{1}{f(p-1)} \sum_{i=1}^{r} \sigma(j_i) d_i \right). \tag{4.16}$$

ACKNOWLEDGMENT

I would like to thank Hendrick Lenstra, Jr., for calling my attention to Moreno-Moreno's work [6, 7] and Ward's work [11], which lead to the present paper, and for pointing out that the Moreno-Moreno theorem does not imply the Ax-Katz theorem. Thanks are also due to the referee for several helpful comments.

REFERENCES

1. A. Adolphson and S. Sperber, *p-adic estimates for exponential sums and the theorem of Chevalley-Warning*, Ann. Sci. École Norm. Sup. (4) **20** (1987), 545–556.
2. ———, *p-adic estimates for exponential sums*, Lecture Notes in Math., vol. 1454, Springer-Verlag, Berlin and New York, 1990, pp. 11–22.
3. J. Ax, *Zeros of polynomials over finite fields*, Amer. J. Math. **86** (1964), 255–261.
4. N. M. Katz, *On a theorem of Ax*, Amer. J. Math. **93** (1971), 485–499.
5. R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia Math Appl., vol. 20, Addison-Wesley, Reading, MA, 1983.
6. O. Moreno and C. J. Moreno, *Improvements of the Chevalley-Warning and the Ax-Katz theorem*, Amer. J. Math. (to appear).
7. ———, *The MacWilliams-Sloane conjecture on the tightness of the Carlitz-Uchiyama bound and the weights of duals of BCH codes*, IEEE Trans. Inform. Theory (to appear).
8. W. M. Schmidt, *Equations over finite fields*, Lecture Notes in Math., vol. 536, Springer-Verlag, Berlin and New York, 1976, p. 135.
9. S. Sperber, *On the p-adic theory of exponential sums*, Amer. J. Math. **108** (1986), 255–296.
10. D. Wan, *An elementary proof of a theorem of Katz*, Amer. J. Math. **111** (1989), 1–8.
11. H. N. Ward, *Weight polarization and divisibility*, Discrete Math. **83** (1990), 315–326.

DEPARTMENT OF MATHEMATICAL SCIENCES, UNIVERSITY OF NEVADA-LAS VEGAS, LAS VEGAS, NEVADA 89154

E-mail address: dwan@nevada.edu