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 $F_q$ 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 $F_q$. The classical Chevalley-Warning theorem asserts that if $n > \sum d_i$, then the characteristic $p$ divides the number $N_q(F_1, \ldots, F_r)$ of $F_q$-rational solutions of the system

$$F_1(x_1, \ldots, x_n) = F_2(x_1, \ldots, x_n) = \cdots = F_r(x_1, \ldots, x_n) = 0.$$  

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

$$N_q(F_1, \ldots, F_r) \equiv \sum_{x \in F_q^n} (1 - F_1(x)^{q-1}) \cdots (1 - F_r(x)^{q-1}) \pmod{p},$$

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

$$b > \frac{n - \sum d_i}{\max d_i},$$

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 $(n - \sum d_i)/\sum d_i$. 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.

©1994 American Mathematical Society

0002-9939/94 $1.00 + .25 per page

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
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 \( F_q \) to the prime field \( F_p \). 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

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

where \( T_q \) is the Teichmüller lifting of \( F_q \) and \( F(x) \) has \( p \)-adic coefficients. Note that \( \lim_{k \to \infty} a^{q^k} \) is simply the Teichmüller lifting of \( a \in F_q \). 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 \( F_i(x_1, \ldots, x_n) \) \( (1 \leq i \leq r) \) 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

\[
F_1(x_1, \ldots, x_n) \equiv F_2(x_1, \ldots, x_n) \equiv \cdots \equiv F_1(x_1, \ldots, x_n) \equiv 0 \pmod{p}.
\]

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 $g^{ip^n}$ $(0 \leq i \leq p-2)$, 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:

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

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

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

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

$$ (2.4) \quad A = \sum_{k_{i_1}, \ldots, k_{i_r} = (p-1)p^n} \prod_{i=1}^{r} \left( \frac{(p-1)p^n}{k_{i_1}, \ldots, k_{i_m}} \right) \left( \prod_{i=1}^{r} \prod_{j=1}^{m_i} a_{ij} \right) \sum_{x \in S^n} \prod_{i<j} (k_{ij} - \sigma(k_{ij})). $$

By the classical formula of Legendre, $\text{ord}_p(k!) = (k - \sigma(k))/(p - 1)$, 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:

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

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

$$ (2.6) \quad \sum_{i,j} k_{ij} e_{ij} \equiv 0 \quad (\text{mod } (p-1)), $$

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 $N_p(F_1, \ldots, F_r)$ is an integer)

$$ (2.7) \quad \frac{n - \sum_i d_i}{\max_i d_i} \leq \frac{1}{p-1} \sum_{i=1}^{r} \left( \sum_{j=1}^{m_i} \sigma(k_{ij}) - (p-1) \right) + (n - s). $$
Since \( k \equiv \sigma(k) \pmod{(p-1)} \), we can replace \( k_{ij} \) by \( \sigma(k_{ij}) \) in (2.6):

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

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

\[
(2.9) \quad s(p-1) - (p-1) \sum_{i=1}^{r} d_i \leq \sum_{i=1}^{r} d_i \left( \sum_{j=1}^{m_i} \sigma(k_{ij}) - (p-1) \right)
\]

\[
\leq d \sum_{i=1}^{r} \left( \sum_{j=1}^{m_i} \sigma(k_{ij}) - (p-1) \right).
\]

This inequality implies that

\[
\frac{1}{p-1} \sum_{i=1}^{r} \left( \sum_{j=1}^{m_i} \sigma(k_{ij}) - (p-1) \right) + (n-s) \geq \left( \frac{s - \sum_{i} d_i}{d} \right) + (n-s) \geq \left( \frac{n - \sum_{i} d_i}{d} \right).
\]

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

### 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 \( \mathbb{Q}_p \). 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 \( \mathbb{F}_q \). Let \( T \) be the Teichmüller character, i.e., \( T(\bar{t}) = \bar{t} \). This is a primitive multiplicative character on \( \mathbb{F}_q \) of order \( (q-1) \). Any multiplicative character of \( \mathbb{F}_q \) is a power of \( T \). Let \( \chi_i(t) = T(t)^{j_i} \) \((1 \leq i \leq r)\) be multiplicative characters of \( \mathbb{F}_q \), where the \( j_i \) are integers satisfying \( 0 \leq j_i \leq q-1 \). By convention, \( T^0(a) \) is the character with value 1 for all \( a \in \mathbb{F}_q \); while \( T^{q-1}(a) \) is the character with value 1 for all \( a \in \mathbb{F}_q^* \) and \( T^{q-1}(0) = 0 \). Let \( F_i(x_1, \ldots, x_n) \) be polynomials of degree \( d_i \) over \( \mathbb{F}_q \). Define a character sum by

\[
(3.1) \quad S_q(\chi, F) = \sum_{x \in \mathbb{F}_q^n} \chi_1(F_1(x)) \cdots \chi_r(F_r(x)).
\]

For an integer \( k \geq 0 \), 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

\[
(3.2) \quad \frac{1}{f} \sum_{a=0}^{f-1} \left( n - \frac{1}{q-1} \sum_{i=1}^{r} \sigma_q(p^a j_i) d_i \right)^*.
\]
Proof. To simplify notation, suppose that the \( F_i(x) \) are already lifted to \( K_q \). Since \( T(x) \equiv x^{q^n} \pmod{q^n} \) for all integral \( x \in K_q \), similar to (1.2), we have the following congruence formula:

\[
S_q(x, F) \equiv \sum_{x \in T_q} F_1(x)^{j_1 q^n} \cdots F_r(x)^{j_r q^n} \pmod{q^n}.
\]

Let \( F_i(x) = \sum_{j=1}^{m_i} a_{ij} x^{e_{ij}} \), where the \( e_{ij} \) are vectors in \( \mathbb{Z}_{\geq 0} \) 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 \( q^n \):

\[
S_q(x, F) \equiv \sum_{k_{11} + \cdots + k_{im} = j} \prod_{i=1}^{r} \left( k_{1i}^{j_1 q^n} \cdots k_{mi}^{j_m q^n} \right) \sum_{x \in T_q} x^{\sum_{i,j} k_{ij} e_{ij}}.
\]

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

\[
\frac{1}{f(p - 1)} \sum_{i=1}^{r} \left( j_i q^n - \sigma(j_i) - \sum_{j=1}^{m_i} (k_{ij} - \sigma(k_{ij})) \right)
\]

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

By the definition of \( T_q \), the following is valid:

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

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

\[
\sum_{i,j} k_{ij} e_{ij} \equiv 0 \pmod{(q - 1)},
\]

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

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

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

\[
s(q - 1) - \sum_{i=1}^{r} j_i d_i \leq \sum_{i=1}^{r} d_i \left( \sum_{j=1}^{m_i} \sigma_q(k_{ij}) - j_i \right) \leq d \sum_{i=1}^{r} \left( \sum_{j=1}^{m_i} \sigma_q(k_{ij}) - j_i \right).\]
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 $i$,
\begin{equation}
\sum_j \sigma_q(k_{ij}) - j_i \equiv 0 \pmod{(q - 1)}.
\end{equation}

It then follows from (3.9) and (3.10) that
\begin{equation}
\left( s - \frac{1}{q-1} \sum_i j_i d_i \right)^* (q - 1) \leq \sum_{i=1}^r \left( \sum_{j=1}^{m_i} \sigma_q(k_{ij}) - j_i \right).
\end{equation}

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
\begin{equation}
\left( s - \frac{1}{q-1} \sum_i \sigma_q(p^a j_i) d_i \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).
\end{equation}

Adding equation (2.12) for $a = 0, 1, \ldots, f - 1$, we deduce that
\begin{equation}
\sum_{a=0}^{f-1} \left( s - \frac{1}{q-1} \sum_i \sigma_q(p^a j_i) d_i \right)^* \frac{q - 1}{p - 1} \sum_{i=1}^r \left( \sum_{j=1}^{m_i} \sigma(k_{ij}) - \sigma(j_i) \right),
\end{equation}
where we used the simple fact that for all integers $k \geq 0$,
\begin{equation}
\sum_{a=0}^{f-1} \sigma_q(p^a k) = \sigma(k) \frac{q - 1}{p - 1}.
\end{equation}

By (3.5) and (3.6), we conclude that the $q$-order of each term in (3.4) is at least
\begin{equation}
\min_{0 \leq s \leq n} \left\{ \frac{1}{f} \sum_{a=0}^{f-1} \left( s - \frac{1}{q-1} \sum_i \sigma_q(p^a j_i) d_i \right)^* + (n - s) \right\}
= \frac{1}{f} \sum_{a=0}^{f-1} \left( n - \frac{1}{q-1} \sum_i \sigma_q(p^a j_i) d_i \right)^*.
\end{equation}

The theorem is proved.

If we take the $\chi_i$ 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
\begin{equation}
N_q(F_1, \ldots, F_r) = \sum_{x \in F_q^r} (1 - \chi_1(F_1(x))) \cdots (1 - \chi_r(F_r(x))).
\end{equation}

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

\[
1 \left( nf - \frac{1}{p-1} \sum_i \sigma(j_i)d_i \right)^*.
\]

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 $\chi_i = T^{j_i}$ ($1 \leq i \leq r$) be multiplicative characters of $F_q$ as above. Let $\psi$ be a fixed nontrivial additive character of $F_q$. Let $F_i(x_1, \ldots, x_n)$ ($1 \leq i \leq r + 1$) be polynomials of degree $d_i$ over $F_q$. Define a mixed character sum by

\[
S_q(\chi, \psi, F) = \sum_{x \in F_q^n} \chi_1(F_1(x)) \cdots \chi_r(F_r(x)) \psi(F_{r+1}(x)).
\]

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

\[
h_i = \max_{(k_1, \ldots, k_n)} \sigma(k_1) + \cdots + \sigma(k_n),
\]

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

\[
f \left( n - \frac{1}{f(p-1)} \sum_{i=1}^{r} \sigma(j_i)h_i \right).
\]

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

\[
S_q(\chi, \psi, F) \equiv \sum_{x \in T_q^n} F_1(x)^{j_1q^n} \cdots F_r(x)^{j_rq^n} \psi(F_{r+1}(x)) \quad (mod \ p^n),
\]

where for simplicity, $\psi(F_{r+1}(x))$ means the value of $\psi$ 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 $T_q^n$. Choose elements $\alpha_1, \ldots, \alpha_f$ in $T_q$ such that their reduction is a basis of $F_q$ over $F_p$. Then every element $x_i$ of $T_q$ can be uniquely written in the form $x_i \equiv y_{i1}\alpha_1 + \cdots + y_{if}\alpha_f \quad (mod \ p)$, where the $y_{ij}$ are elements in $T_p$. Let $k = k_0 + k_1p + k_2p^2 + \cdots$ be a positive integer. Then

\[
x_i^k \equiv \left( \sum_{j=1}^{f} y_{ij}\alpha_j \right)^{k_0 + k_1p + k_2p^2 + \cdots}
\]

\[
\equiv \left( \sum_{j=1}^{f} y_{ij}\alpha_j \right)^{k_0} \left( \sum_{j=1}^{f} y_{ij}\alpha_j^p \right)^{k_1} \cdots \quad (mod \ p).
\]

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 $K_q[y_{11}, y_{12}, \ldots, y_{nf}]$ 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 $\psi(G_{r+1}(y)) = \psi_p(\text{tr}(G_{r+1}(y))) = \psi_p(G'_{r+1}(y))$, where $\psi_p$ is an additive character $\psi_p$ of $F_p$ and the polynomial $G'_{r+1}(y)$ has coefficients in $Z_p$. For each $1 \leq i \leq r$, 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 $F_i'(x)$ (coming from $\chi_i(F_i) = T(F_i')$) by a product polynomial $U_i G_{ik}^x(y)$, where each $G_{ik}$ is a $p$-adic integral polynomial in $K_q[yx_1, yx_2, \ldots, yx_n]$ 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 $F_i(x)$ ($1 \leq i \leq r$) may have coefficients in the extension $K_q$. Namely, we are reduced to consider

\begin{equation}
S_p(\chi, \psi, F) \equiv \sum_{x \in T_p^p} F_1(x)^{j_1p^n} \cdots F_r(x)^{j_rp^n} \psi_p(F_{r+1}(x)) \pmod{p^n},
\end{equation}

where $0 \leq j_i \leq p - 1$, 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 $Z_p$. We need to prove that the $p$-order of the sum in (4.5) is at least

\begin{equation}
\frac{1}{\max_{1 \leq i \leq r+1} d_i} \left( n - \frac{1}{(p-1)} \sum_i j_i d_i \right).
\end{equation}

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

\begin{equation}
\prod_{i=1}^{r} F_i(x)^{j_ip^n} = \sum_{k_1 + \cdots + k_{m_i} = j_i p^n} \prod_{i=1}^{r} \left( k_i p^n \right) \left( \prod_{j=1}^{m_i} a_{ij}^x \right)^{x e_{ij}}.
\end{equation}

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

\begin{equation}
\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),
\end{equation}

For the additive part, we use Gauss sums and Stickelberger's theorem. For integer $k$ with $0 \leq k \leq p - 2$, define the Gauss sum $g_k = \sum_{x \in T_p} \psi_p(x) e^k x$.

\begin{equation}
\psi_p(\tilde{t}) = \sum_{k=0}^{p-1} G(k)t^k,
\end{equation}

for all $t \in T_p$. One checks that $G(0) = 1$, $G(p-1) = -p/(p-1)$ and for $1 \leq k \leq p - 2$, $G(k) = g_k/(p-1)$. 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 $0 \leq k \leq p - 1$. For simplicity,
we define \( \psi_p(x) = \psi_p(\bar{x}) \) if \( x \) is a \( p \)-adic integer in \( \mathbb{Z}_p \). Using (4.9), for all \( x \in T_p^n \) we have the expansion

\[
\psi_p(F_{r+1}(x)) = \prod_{j=1}^{m} \psi_p(b_j x^{e_j})
\]

(4.10)

\[
= \prod_{l_i, \ldots, l_m = 0}^{p-1} \left( \prod_{j=1}^{m} G(l_j) \right) \prod_{j=1}^{m} (b_j x^{e_j})^{l_j}
\]

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

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

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

(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 \( d = \max_{1 \leq i \leq r+1} d_i \). By the above computation, we are reduced to proving that

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

(4.12)

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

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

(4.13)

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

\[
s(p - 1) - \sum_{i=1}^{r} j_i d_i \leq \sum_{i=1}^{r} d_i \left( \sum_{j=1}^{m_i} \sigma(k_{ij}) - j_i \right) + \sum_{j=1}^{m} l_j d_{r+1}
\]

(4.14)

\[
\leq d \left( \sum_{i=1}^{r} \left( \sum_{j=1}^{m_i} \sigma(k_{ij}) - j_i \right) + \sum_{j=1}^{m} l_j \right).
\]

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

\[
\frac{1}{p - 1} \left( \sum_{i=1}^{r} \left( \sum_{j=1}^{m_i} \sigma(k_{ij}) - j_i \right) + \sum_{j=1}^{m} l_j \right) + (n - s)
\]

\[
\geq \left( s - \frac{1}{p - 1} \sum_{i=1}^{r} j_i d_i \right) + (n - s) \geq \frac{1}{d} \left( n - \frac{1}{p - 1} \sum_{i=1}^{r} j_i d_i \right).
\]

Theorem 4.1 is proved.
If we take the $\chi_i$ to be the characters with $j_i = 0$ and take $F_i$ with $d_i = 1$ for all $i \leq r$, then

$$S_q(\chi, \psi, F) = S_q(\psi, F_{r+1}) = \sum_{x \in F_q^*} \psi(F_{r+1}(x))$$

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 $f n / h_{r+1}$. 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

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

**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**


Department of Mathematical Sciences, University of Nevada-Las Vegas, Las Vegas, Nevada 89154

E-mail address: dwan@nevada.edu