Exponential sums over finite fields

Harald Niederreiter*
EXPONENTIAL SUMS OVER FINITE FIELDS

HARALD NIEDERREITER

Let \( F_q \) be the finite field of order \( q \). For \( f \in F_q[x_1,\ldots,x_r] \) and a nontrivial additive character \( \chi \) of \( F_q \), define the character sum

\[
C_1 = \sum_{a_1,\ldots,a_r \in F_q} \chi(f(a_1,\ldots,a_r)).
\]

Together with \( C_1 \) we consider lifted character sums corresponding to the various finite extensions \( F_{q^r} \) of \( F_q \) contained in a fixed algebraic closure \( \overline{F}_q \) of \( F_q \). First, \( \chi \) is lifted via the trace to a nontrivial additive character \( \chi^{\text{Tr}} \) of \( F_{q^r} \); in detail, if \( \text{Tr}_r \) denotes the trace function from \( F_{q^r} \) onto \( F_q \), then set

\[
(1) \quad \chi^{\text{Tr}}(a) = \chi(\text{Tr}_r(a)) \text{ for } a \in F_{q^r}.
\]

Now define

\[
C_s = \sum_{a_1,\ldots,a_r \in F_{q^s}} \chi^{\text{Tr}}(f(a_1,\ldots,a_r)).
\]

With these lifted character sums one sets up the \( L \)-function

\[
L(z) = \exp \left( \sum_{s=1}^{\infty} \frac{C_s}{s} z^s \right)
\]

in the complex variable \( z \). For \( r = 1 \) one has the classical results of A. Weil on these \( L \)-functions (see [5, Ch. 5]). For general \( r \), Grothendieck [4] proved by methods of \( l \)-adic cohomology that \( L(z) \) is always a rational function. Bombieri [1] conjectured that \( L(z) \) has the special form

\[
(2) \quad L(z) = P(z)^{-1} \zeta^{-1}
\]

with a polynomial \( P \), provided that \( f \) satisfies some kind of nonsingularity condition. In his famous paper on the Weil conjectures, Deligne [3] proved among other results that Bombieri's conjecture is true if \( \text{deg}(f) \) is not a multiple of the characteristic of \( F_q \) and the leading homogeneous part \( f_0 \) of \( f \) is nonsingular in the standard sense (i.e., there is no point over \( \overline{F}_q \) at which \( f_0 \) and all its first-order partial derivatives vanish simultaneously).

In a lecture given at the Oberwolfach Conference on Analytic Number Theory in 1982, S. A. Stepanov announced an elementary proof of the result of Deligne quoted above for the case where \( \text{deg}(f) \) is less than the charac-
teristic of $F_q$ (see [12]). According to the outline given by Stepanov, his method depends, first of all, on an explicit expansion of $L(z)$, where we assume for simplicity that $r$ is odd (otherwise consider $L(z)^{-1}$):

$$L(z) = \exp \left( \sum_{s=1}^{\infty} \frac{C_s}{s} z^s \right) = \prod_{s=1}^{\infty} \exp \left( \frac{C_s}{s} z^s \right) = \prod_{s=1}^{\infty} \left( \sum_{i=0}^{\infty} \frac{1}{i!} \cdot \frac{C_{s_i}^{i_j}}{i_1 \cdots i_s} \cdot \frac{C_{s_0}^{i_0}}{2^{i_1} \cdots s_{i_s}^i} \right) z^s = 1 + \sum_{s=1}^{\infty} a_s z^s.$$

Now one has to show $a_s = 0$ for all sufficiently large $s$. Stepanov claimed that he can do this by inserting the explicit form of the sums $C_i$, then fully expanding the resulting expression for $a_s$ and combining terms in a suitable way. In a brief note [13] summarizing the method, this point is brushed over. Since I could not get any further details from Stepanov, I tried to reconstruct his argument and I looked first for a simple test case.

It turns out that Stepanov had already used this method in his paper [11] to give an elementary proof of the Davenport-Hasse theorem for Gaussian sums over finite fields. A closer inspection of this proof reveals, however, that it breaks down at a crucial step of the argument. This raises some doubts about the validity of Stepanov's claim at the Oberwolfach conference. But, obviously, a final verdict can only be given when Stepanov publishes his proof in full detail.

In order to elaborate on the error in [11], it is necessary to first describe the Davenport-Hasse theorem. Let $\psi$ be a multiplicative and $\chi$ an additive character of $F_q$, not both being trivial, and use the convention $\psi(0) = 0$. The corresponding Gaussian sum is defined by

$$G_t = G(\psi, \chi) = \sum_{a \in F_q^*} \psi(a) \chi(a).$$

The character $\psi$ is lifted by means of the formula

$$\psi^{[g]}(a) = \psi(N_s(a)) \quad \text{for} \quad a \in F_q^*,$$

where $N_s$ is the norm function from $F_q^*$ onto $F_q$. With $\chi^{[g]}$ being given by (1), we consider the lifted Gaussian sum

$$G_s = G(\psi^{[g]}, \chi^{[g]}) = \sum_{a \in F_q^*} \psi^{[g]}(a) \chi^{[g]}(a).$$

The Davenport-Hasse theorem expresses the following simple relation between $G_s$ and $G_t$. 

http://escholarship.lib.okayama-u.ac.jp/mjou/vol27/iss1/21
Davenport-Hasse Theorem. \( G_s = (-1)^{s-1} G_1^s \).

In the paper of Davenport and Hasse [2] this relation arose from the study of \( L \)-functions of an algebraic function field defined by an Artin-Schreier curve over \( \mathbb{F}_q \). The paper contains also a proof of the formula based on the results of Stickelberger [14] concerning the factorization of Gaussian sums in cyclotomic fields. Schmid [10] has given an elementary proof of the Davenport-Hasse theorem by induction on \( s \).

Although this is not made explicit, the method in Stepanov [11] for proving the Davenport-Hasse theorem amounts to considering an \( L \)-function corresponding to Gaussian sums and expanding it as in (3):

\[
L(z) = \exp \left( \sum_{s=1}^{\infty} \frac{G_s}{s} z^s \right) = 1 + \sum_{s=1}^{\infty} \gamma_s z^s
\]

with

\[
\gamma_s = \sum_{i_1 + 2i_2 + \cdots + si_s = s} \frac{G_1^{i_1} \cdots G_s^{i_s}}{i_1! i_s! 2^{i_2} \cdots s^{i_s}}.
\]

Then one tries to show \( \gamma_s = 0 \) for \( s > 1 \). In one of the key steps it is claimed in [11] that for a given solution of \( i_1 + 2i_2 + \cdots + si_s = s \) in non-negative integers \( i_1, \cdots, i_s \), the number \( N(t_1, \cdots, t_s) \) of tuples

\[
(a_1^{(1)}, \cdots, a_i^{(1)}, \cdots, a_s^{(1)}, \cdots, a_i^{(s)}),
\]

with the first \( i_1 \) entries being in \( \mathbb{F}_q \), the next \( i_2 \) entries being in \( \mathbb{F}_{q^2} \), \( \cdots \), the last \( i_s \) entries being in \( \mathbb{F}_{q^s} \), and with the elementary symmetric polynomials in the \( a_i^{(i)} \) and their conjugates over \( \mathbb{F}_q \) having prescribed values \( t_1, \cdots, t_s \in \mathbb{F}_q \), is independent of \( t_1, \cdots, t_s \). This statement is, however, incorrect. For instance, if \( i_s = 0 \) and

\[
t(x) = x^s - t_1 x^{s-1} + t_2 x^{s-2} \mp \cdots + (-1)^s t_s
\]

is irreducible over \( \mathbb{F}_q \), then \( N(t_1, \cdots, t_s) = 0 \), whereas \( N(0, \cdots, 0) = 1 \), as can be seen immediately from the factorization of \( t(x) \) in its splitting field over \( \mathbb{F}_q \). To provide another counterexample, we note that if \( i_1 = s \), \( i_2 = \cdots = i_s = 0 \), then \( N(t_1, \cdots, t_s) = 0 \) whenever \( t(x) \) does not split completely over \( \mathbb{F}_q \), whereas \( N(0, \cdots, 0) = 1 \) and \( N(1, 0, \cdots, 0) = s \). The proof of the Davenport-Hasse theorem in [11] is therefore fallacious. Any attempt to repair it would have to be based on a correct formula for \( N(t_1, \cdots, t_s) \). Such a formula will, however, be very complicated and lead to a rather involved
proof of the Davenport-Hasse theorem.

We present now a short proof of the Davenport-Hasse theorem using a technique in [5, Ch. 5]. Let \( M = \{ g \in \mathbb{F}_q[x] : g \text{ monic} \}, M_r = \{ g \in M : \deg(g) = r \}, I = \{ g \in M : g \text{ irreducible over } \mathbb{F}_q \}, I_a = \{ g \in I : \deg(g) = d \}. \) Define \( \lambda : M \to \mathbb{C} \) by \( \lambda(1) = 1 \) and

\[
\lambda(x^r - c_1 x^{r-1} + \cdots + (-1)^r c_r) = \varphi(c_r) \chi(c_1) \text{ for } r \geq 1.
\]

Then \( \lambda \) is multiplicative in the sense that \( \lambda(gh) = \lambda(g) \lambda(h) \) for all \( g, h \in M \). Splitting up \( G_s \) according to the degree of \( a \in \mathbb{F}_q^* \) over \( \mathbb{F}_q \), writing \( g_a \) for the minimal polynomial of \( a \) over \( \mathbb{F}_q \), and using simple properties of \( \text{Tr}_s \) and \( N_s \) (see [5, Ch. 2]), we get for \( |z| < q^{-1/2} \):

\[
\sum_{s=1}^{\infty} \frac{G_s}{s} z^s \sum_{d=1}^{\infty} \frac{1}{d} \sum_{a \in \mathbb{F}_q^*} g_a^{a/d} \lambda(g_a)^{a/d} = \sum_{s=1}^{\infty} \frac{1}{s} \sum_{d=1}^{\infty} \frac{1}{d} \sum_{a \in \mathbb{F}_q^*} g_a^{a/d} \lambda(g_a)^{a/d} = \sum_{s=1}^{\infty} \frac{1}{s} \sum_{d=1}^{\infty} \frac{1}{d} \sum_{a \in \mathbb{F}_q^*} g_a^{a/d} \lambda(g_a)^{a/d} = \prod_{a \in \mathbb{F}_q^*} \frac{1}{1 - \lambda(g_a) z^{d_{\deg(a)}}}.
\]

In this Euler product \( \lambda(g) z^{d_{\deg(a)}} \) is multiplicative as a function of \( g \), hence

\[
\sum_{s=1}^{\infty} \frac{G_s}{s} z^s = \log \left( \sum_{a \in M} \lambda(g) z^{d_{\deg(a)}} \right) = \log \left( \sum_{r=0}^{\infty} \left( \sum_{g \in M_r} \lambda(g) \right) z^r \right) = \log (1 + G_1 z) = \sum_{s=1}^{\infty} \frac{1}{s} (-1)^{s-1} G_1^s z^s,
\]

and comparison of coefficients yields the Davenport-Hasse theorem.

The same method can be applied to other exponential sums. For instance, if \( \psi_1 \) and \( \psi_2 \) are two multiplicative characters of \( \mathbb{F}_q \), not both of them trivial, and if we fix a nonzero \( b \in \mathbb{F}_q \), then we can consider the lifted Jacobi sums

\[
J_s = \sum_{a \in \mathbb{F}_q^*} \psi_1^{[s]}(a) \psi_2^{[s]}(b - a).
\]
EXponential Sums Over Finite Fields

With

\[ \lambda(g) = \phi((-1)^{\deg g}g(0)) \psi(g(b)) \] for \( g \in M \)

we get then as above:

\[
\sum_{s=1}^{\infty} \frac{J_s}{s} z^s = \log \left( \sum_{r=0}^{\infty} \left( \sum_{g \in M_r} \lambda(g) \right) z^r \right) \\
= \log(1 + J_0 z) = \sum_{s=1}^{\infty} \frac{1}{s} (-1)^{s-1} J_s^0 z^s,
\]

and comparison of coefficients yields \( J_s = (-1)^{s-1} J_s^0 \), a formula first shown by Mitchell [6].

The Davenport-Hasse theorem can be used to establish a formula of the type (2) for \( L \)-functions corresponding to a general class of multiple exponential sums. For \( 1 \leq i \leq r \) let \( F_i \) be a finite field, let \( \chi_i \) be a nontrivial additive character of \( F_i \), and let \( \psi_i \) be an arbitrary multiplicative character of \( F_i \). Let \( H_i \) be a subgroup of the direct product \( F_1^\ast \times \cdots \times F_r^\ast \) of index \( m \), where \( F_i^\ast \) denotes the multiplicative group of a finite field \( F \). If \( F_{i,s} \) is the extension of \( F_i \) of degree \( s \) contained in a fixed algebraic closure of \( F_i \), let

\[
\overline{N}_s : F_{1,s}^\ast \times \cdots \times F_{r,s}^\ast \to F_1^\ast \times \cdots \times F_r^\ast
\]

be the componentwise norm function and set \( H_s = \overline{N}_s^{-1}(H_i) \). For fixed \( u \in F_1^\ast \times \cdots \times F_r^\ast \) define

\[
E_s = m \sum_{(a_1, \ldots, a_r) \in H_s} \chi_1^{(a_1)}(a_1) \cdots \chi_r^{(a_r)}(a_r) \psi_1^{(a_1)}(a_1) \cdots \psi_r^{(a_r)}(a_r).
\]

Then set up the corresponding \( L \)-function

\[
L(z) = \exp \left( \sum_{s=1}^{\infty} \frac{E_s}{s} z^s \right).
\]

**Theorem 1.** The \( L \)-function in (5) is of the form

\[
L(z) = P(z)^{-1} z^{-1}
\]

with a polynomial \( P \) of degree \( m \) satisfying \( P(0) = 1 \).

**Proof.** If \( u = (u_1, \ldots, u_r) \in F_1^\ast \times \cdots \times F_r^\ast \), we can write

\[
E_s = m \sum_{(u_1, \ldots, u_r) \in H_s} \chi_1^{(u_1)}(u_1) \cdots \chi_r^{(u_r a_r)}(u_r a_r) \psi_1^{(u_1)}(a_1) \cdots \psi_r^{(u_r a_r)}(u_r a_r).
\]

For fixed \( s \) we use the Fourier expansion of the restriction of \( \chi_i^{(a_i)} \) to \( F_{i,s}^\ast \) with
respect to the characters \( \lambda_t \) of that group:

\[
\chi_t^{(s)}(c) = \frac{1}{q_t^{s} - 1} \sum_{\lambda_t} G(\tilde{\lambda}_t, \chi_t^{(s)}) \lambda_t(c) \text{ for all } c \in F_t^{*s},
\]

where \( q_t \) denotes the order of \( F_t \); the Fourier coefficients are Gaussian sums; and \( \tilde{\lambda}_t \) is the conjugate character of \( \lambda_t \). Inserting (7) in (6) we get

\[
E_s = \frac{m}{(q_t^s - 1) \cdots (q_r^s - 1)} \sum_{\lambda_t, \lambda_r \in H_t} \phi_t^{(s)}(u_1 a_1) \cdots \phi_r^{(s)}(a_r u_r) \cdot \\
\sum_{\lambda_t, \lambda_r} G(\tilde{\lambda}_t, \chi_t^{(s)}) \cdots G(\tilde{\lambda}_r, \chi_r^{(s)}) \lambda_t(u_1 a_1) \cdots \lambda_r(u_r a_r)
\]

\[
= \frac{m}{(q_t^s - 1) \cdots (q_r^s - 1)} \sum_{\lambda_t, \lambda_r \in H_t} \phi_t^{(s)}(u_r) \sum_{\lambda_t, \lambda_r} (\phi_t^{(s)}(\lambda_t)(a_1) \cdots (\phi_r^{(s)}(\lambda_r)(a_r)).
\]

Let \( A_s \) be the annihilator of \( H_s \) in the dual group of \( F_1^{*s} \times \cdots \times F_r^{*s} \). Then the inner sum has the value \( |H_s| \) if \((\phi_t^{(s)}(\lambda_t), \cdots, \phi_r^{(s)}(\lambda_r) \in A_s \) and 0 otherwise. Therefore,

\[
E_s = \frac{m}{(q_t^s - 1) \cdots (q_r^s - 1)} \sum_{\lambda_t, \lambda_r \in A_s} G(\tilde{\lambda}_t, \phi_t^{(s)}) \cdots G(\tilde{\lambda}_r, \phi_r^{(s)}) \lambda_t(u_1) \cdots \lambda_r(u_r).
\]

Since \( \tilde{N}_s \) is surjective, we have

\[
|\ker \tilde{N}_s| = \frac{(q_1^s - 1) \cdots (q_r^s - 1)}{(q_1 - 1) \cdots (q_r - 1)},
\]

and from \( H_1 \cong H_s/\ker \tilde{N}_s \) we get

\[
|H_s| = |H_1| \frac{(q_1^s - 1) \cdots (q_r^s - 1)}{(q_1 - 1) \cdots (q_r - 1)}.
\]

This implies

\[
|A_s| = \frac{|A_1|}{|H_s|} = \frac{(q_1 - 1) \cdots (q_r - 1)}{(q_1^s - 1) \cdots (q_r^s - 1)} = |A_1|.
\]

Since it is immediate that \((\lambda_1^{(s)}, \cdots, \lambda_r^{(s)}) \in A_s \) whenever \((\lambda_1, \cdots, \lambda_r) \in A_1 \), it follows from (10) that \( A_s \) consists exactly of all \((\lambda_1^{(s)}, \cdots, \lambda_r^{(s)}) \) with \((\lambda_1, \cdots, \lambda_r) \in A_1 \). Using this fact as well as (9) and the definition of \( m \), the identity (8) attains the form
EXPONENTIAL SUMS OVER FINITE FIELDS

\[ E_s = \sum_{A_1, \ldots, A_r \in A_i} G(\tilde{\lambda}_1^{(s)}, \chi_1^{(s)}) \cdots G(\tilde{\lambda}_r^{(s)}, \chi_r^{(s)}) \lambda_1^{(s)}(u_1) \cdots \lambda_r^{(s)}(u_r). \]

Now we can apply the Davenport-Hasse theorem, and taking into account that \( \tilde{\lambda}_i^{(s)}(u_i) = (\lambda_i(u_i))^s \), we get

\[ E_s = (-1)^r \sum_{A_1, \ldots, A_r \in A_i} ((-1)^r G(\tilde{\lambda}_1^{(s)}, \chi_1) \cdots G(\tilde{\lambda}_r^{(s)}, \chi_r) \lambda_1(u_1) \cdots \lambda_r(u_r))^s. \]

Since \(|A_i| = m\), we can label the numbers

\[ (11) \quad (-1)^r G(\tilde{\lambda}_1, \chi_1) \cdots G(\tilde{\lambda}_r, \chi_r) \lambda_1(u_1) \cdots \lambda_r(u_r) \]

by \( \omega_1, \ldots, \omega_m \), so that

\[ (12) \quad E_s = (-1)^r \sum_{j=1}^{m} \omega_j^s. \]

For the \( L \)-function in (5) we obtain then

\[ L(z) = \exp \left( (-1)^r \sum_{j=1}^{m} \frac{z^s}{s} \sum_{j=1}^{m} \omega_j^s \right) = \exp \left( (-1)^r \sum_{j=1}^{m} \sum_{j=1}^{m} \frac{1}{s} (\omega_j z)^s \right) \]

\[ = \exp \left( (-1)^{r-1} \sum_{j=1}^{m} \log (1 - \omega_j z) \right) = P(z)^{r-1}. \]

with

\[ P(z) = (1 - \omega_1 z) \cdots (1 - \omega_m z). \]

Since the characters \( \chi_i \) are nontrivial, we have \( \omega_j \neq 0 \) for \( 1 \leq j \leq m \), and the proof of Theorem 1 is complete.

The exponential sums in (4) include various classical exponential sums as special cases, such as Gaussian sums, Kummer cyclotomic periods, and products of such sums. They also include a class of character sums studied by the author in a number of papers (see [7], [8], [9]). This will be explained in the sequel.

Let \( (y_n), n = 0, 1, \ldots, \) be a linear recurring sequence in \( \mathbb{F}_q \) satisfying the linear recurrence relation

\[ (13) \quad y_{n+k} = b_{k-1}y_{n+k-1} + \cdots + b_0y_n, \quad n = 0, 1, \ldots, \]

with constant coefficients \( b_{k-1}, \ldots, b_0 \in \mathbb{F}_q \), \( b_0 \neq 0 \). To exclude a trivial case, we assume \( (y_0, \ldots, y_{k-1}) \neq (0, \ldots, 0) \). We can also assume that (13) is the linear recurrence relation of least order satisfied by \( (y_n) \), i.e., that

\[ f(x) = x^k - b_{k-1}x^{k-1} - \cdots - b_0 \in \mathbb{F}_q[x] \]
is the minimal polynomial of \((y_n)\) (compare with \([5, \text{Ch. 8}]\)). Then the least period \(r\) of \((y_n)\) is equal to the least positive integer \(e\) such that \(f(x)\) divides \(x^e - 1\). We consider now the case where \(f\) has no multiple roots. Then

\[ f = f_1 \cdots f_r \]

with distinct monic irreducible polynomials \(f_i\) over \(K = \mathbb{F}_q\). Let \(\nu_i\) be a fixed root of \(f_i\) in its splitting field \(F_i\) over \(K\), and let \(\text{Tr}_{F_i/K}\) denote the trace function from \(F_i\) onto \(K\).

**Lemma.** Under the conditions above, there exist elements \(u_i \in F_i\), \(1 \leq i \leq r\), such that

\[ y_n = \sum_{i=1}^r \text{Tr}_{F_i/K}(u_i \nu_i^n) \text{ for } n = 0, 1, \ldots. \]

**Proof.** Let

\[ G(x) = \sum_{n=0}^\infty y_n x^n \]

be the generating function of \((y_n)\). On account of the linear recurrence relation, it is of the form

\[ G(x) = \frac{g(x)}{f^* (x)} \]

with \(g \in \mathbb{F}_q[x]\), \(\deg(g) < k\), and \(f^*(x) = x^k f(1/x)\) being the reciprocal polynomial of \(f\) (compare with \([5, \text{Ch. 8}]\)). By partial fraction decomposition,

\[ G(x) = \sum_{i=1}^r \sum_{j=0}^{d_i-1} \frac{a_{ij}}{1 - \nu_i^{q^j} x}, \]

where \(d_i = \deg(f_i)\), and the elements \(a_{ij} \in F_i\) are conjugate over \(K\), i.e., \(a_{ij} = a_{i0}^{q^j}\) for \(0 \leq j \leq d_i - 1\). Expanding into formal power series, we get

\[ G(x) = \sum_{i=1}^r \sum_{j=0}^{d_i-1} a_{ij} \sum_{n=0}^{\infty} \nu_i^{q^j} x^n = \sum_{n=0}^{\infty} \left( \sum_{i=1}^r \sum_{j=0}^{d_i-1} (a_{i0} \nu_i^n)^{q^j} \right) x^n, \]

\[ = \sum_{n=0}^{\infty} \left( \sum_{i=1}^r \text{Tr}_{F_i/K}(a_{i0} \nu_i^n) \right) x^n. \]

and comparison of coefficients with (14) yields the result of the lemma, with \(u_i = a_{i0}\).
Since \( f(0) = -b_0 \neq 0 \), we have \( v_i \neq 0 \) for \( 1 \leq i \leq r \), and since \( f \) is the minimal polynomial of \( (y_n) \), we have \( u_i \neq 0 \) for \( 1 \leq i \leq r \). Now let \( \chi \) be a nontrivial additive character of \( K = \mathbb{F}_q \) and consider the character sum

\[
\sum_{n=0}^{r-1} \chi(y_n)
\]

extended over the period of \( (y_n) \). Then writing again \( d_i = \deg f_i \) and using the lemma,

\[
\sum_{n=0}^{r-1} \chi(y_n) = \sum_{n=0}^{r-1} \chi(\text{Tr}_{\mathbb{F}_q}(u_1 v_n)) \cdots \chi(\text{Tr}_{\mathbb{F}_q}(u_r v_n))
\]

\[
= \sum_{n=0}^{r-1} \chi^{d_1}(u_1 v_n) \cdots \chi^{d_r}(u_r v_n)
\]

\[
= \sum_{(a_1, \ldots, a_r) \in H} \chi^{d_1}(a_1) \cdots \chi^{d_r}(a_r),
\]

where \( u = (u_1, \ldots, u_r) \in F_1^* \times \cdots \times F_r^* \) and \( H_i \) is the cyclic subgroup of \( F_1^* \times \cdots \times F_r^* \) generated by \( (v_1, \ldots, v_r) \). Consequently, the character sum (15) is, apart from the factor \( m \), a sum of the form \( E_1 \) in (4), with \( \chi_i = \chi^{d_i} \) and trivial \( q_i \) for \( 1 \leq i \leq r \).

The identity (12), together with the form of the \( \omega_j \) given by (11), immediately yields the estimate

\[
|E_s| \leq m(q_1 \cdots q_r)^{s/2}
\]

for the sums \( E_s \) in (4), where \( q_i \) denotes the order of \( F_i \). If all \( q_i \) are identical, then we can establish an estimate that is in a sense best possible.

**Theorem 2.** Let \( F_i = \mathbb{F}_q \) for \( 1 \leq i \leq r \). Then there exist integers \( C \) and \( H \) with \( 0 < C \leq m \), \( 0 \leq H \leq r \), such that

\[
|E_s| \leq Cq^{sH/2} + (m-C)q^{sH-1/2} \text{ for all } s \geq 1.
\]

Furthermore, for every \( \epsilon > 0 \) there exist infinitely many \( s \) with

\[
|E_s| \geq (C-\epsilon)q^{sH/2}.
\]

**Proof.** By (12) we have

\[
|E_s| = \left| \sum_{j=1}^{m} \omega_j^s \right|,
\]

where the \( \omega_j \) are given by (11). For \( 0 \leq h \leq r \) let \( m_h \) be the number of
\[ (\lambda_1, \cdots, \lambda_r) \in A_i \text{ such that } \lambda_i = \phi_i \text{ holds for exactly } h \text{ values of } i. \text{ Then} \]

\[ (16) \quad \sum_{h=0}^{r} m_h = m. \]

We note the fact that for a multiplicative character \( \psi \) and a nontrivial additive character \( \chi \) of \( \mathbb{F}_q \) we have

\[ |G(\psi, \chi)| = \begin{cases} 1 & \text{for } \psi \text{ trivial,} \\ q^{1/2} & \text{otherwise.} \end{cases} \]

Therefore,

\[ (17) \quad |E_s| \leq \sum_{h=0}^{r} m_h q^{s(H-h)/2}. \]

Let \( H \) be the largest value of \( h \) with \( m_{r-h} \neq 0 \). Putting \( C = m_{r-h} \), we get

\[ |E_s| \leq Cq^{sh/2} + (m-C)q^{(sh-1)/2} \text{ for all } s \geq 1, \]

where we used (16).

To prove the second part of Theorem 2, let \( \varepsilon > 0 \) be given and let \( J \) be the set of those \( j, 1 \leq j \leq m \), for which \( |\omega_j| = q^{n/2} \). For \( j \in J \) we have

\[ \omega_j = q^{n/2} e^{2\pi i \theta_j} \text{ with } \theta_j \text{ real.} \]

We note that the set \( J \) has \( C \) elements. Therefore, by Dirichlet's theorem on simultaneous diophantine approximations, there exist infinitely many \( s \) for which

\[ \left| \sum_{j \in J} e^{2\pi i s \theta_j} \right| \geq C - \frac{\varepsilon}{2}. \]

Consequently,

\[ |E_s| \geq \left| \sum_{j \in J} \omega_j \right|^2 \geq q^{sH/2} \left| \sum_{j \in J} e^{2\pi i s \theta_j} \right| \geq \left( C - \frac{\varepsilon}{2} \right) q^{sH/2} - (m-C)q^{(sH-1)/2} \geq (C - \varepsilon)q^{sH/2} \]

for infinitely many \( s \).

An interesting special case for applications is that of the character sums in (15), with the minimal polynomial \( f \) of \( \langle y_n \rangle \) being irreducible over \( \mathbb{F}_q \). In this case \( r = 1 \), \( F_1 = \mathbb{F}_r^* \), and \( H_1 \) is the subgroup of \( F_t^* \) generated

http://escholarship.lib.okayama-u.ac.jp/mjou/vol27/iss1/21
by a root \( v \) of \( f \), so that \( m = (q^k - 1)/\tau \). By the earlier discussion,

\[
\sum_{n=0}^{\tau-1} \chi(y_n) = \frac{1}{m} E_1
\]

for a sum \( E_1 \) of the form (4) with \( \phi_1 \) trivial. The lifted sum \( E_s \), \( s \geq 2 \), corresponds to a subgroup \( H_s \) of \( F_{q^s}^* \) of the same index \( m \). Now \( H_s \) is cyclic of order \( \tau_s = (q^{ks}-1)/m \), so we can choose a generator \( v^{(s)} \) of \( H_s \). Let \( f^{(s)} \) be the minimal polynomial of \( v^{(s)} \) over \( \mathbb{F}_{q^s} \). It is clear that \( d = \deg(f^{(s)}) \) divides \( k \). Suppose \( d \) is a proper divisor of \( k \). Then it follows that

\[
\tau_s = \frac{(q^{ks}-1)\tau}{q^k-1} = (q^{ks-1} + q^{ks-2} + \cdots + 1)\tau > q^{ks/2} > q^d - 1.
\]

On the other hand, \( v^{(s)} \) is a nonzero element of the finite field of order \( q^d \), hence

\[
(v^{(s)})^{q^d - 1} = 1,
\]

which implies \( \tau_s \leq q^d - 1 \), a contradiction. Thus we have \( \deg(f^{(s)}) = k \).

From the earlier discussion we see that there exists a linear recurring sequence \( (y_n^{(s)}) \) in \( \mathbb{F}_{q^s} \) with minimal polynomial \( f^{(s)} \) and least period \( \tau_s \) such that

\[
\sum_{n=0}^{\tau_s-1} \chi^{(s)}(y_n^{(s)}) = \frac{1}{m} E_s.
\]

For \( s = 1 \) we write \( y_n^{(1)} = y_n \), \( f^{(1)} = f \), and \( \tau_1 = \tau \). From (17) and the second part of Theorem 2 we obtain then the following result.

**Corollary.** For all \( s \geq 1 \) we have

\[
\left| \sum_{n=0}^{\tau_s-1} \chi^{(s)}(y_n^{(s)}) \right| \leq \left( 1 - \frac{\tau_s}{q^{ks}-1} \right) \frac{q^{ks/2} + \frac{\tau_s}{q^k-1}}{q^s-1}.
\]

Furthermore, for every \( \varepsilon > 0 \) there exist infinitely many \( s \) with

\[
\left| \sum_{n=0}^{\tau_s-1} \chi^{(s)}(y_n^{(s)}) \right| \geq \left( 1 - \frac{\tau_s}{q^{ks}-1} - \varepsilon \right) q^{ks/2}.
\]

In case \( \tau_s = q^{ks} - 1 \) (i.e., \( m = 1 \)), the second part of the corollary provides no information. But in this case it is easy to see directly that
H. NIEDERREITER

\[ \sum_{n=1}^{r} \chi^{(s)}(y_n^{(s)}) = -1, \]

and so (18) is again best possible.

REFERENCES

Math. Soc. 17 (1916), 165-177.
[7] H. NIEDERREITER: Some new exponential sums with applications to pseudo-random numbers,
Topics in Number Theory (Debreceen, 1974), Colloquia Math. Soc. János Bolyai, vol. 13,
(1976), 53-77.
Math. Soc. 84 (1978), 957-1041.
[12] S. A. STEPANOV: Exponential sums in several variables and L-functions of Artin, Tagungs-
321-367.

MATHEMATICAL INSTITUTE
AUSTRIAN ACADEMY OF SCIENCES
DR. IGNAZ-SEIPEL-PLATZ 2
A-1010 VIENNA, AUSTRIA

(Received September 15, 1985)

This paper was presented at the "Colloque sur la théorie analytique et élémentaire
des nombres" in Marseille-Luminy (France), May 30 - June 3, 1983.