Mathematical Journal of Okayama University

Volume 27, *Issue* 1 1985 *Article* 21

JANUARY 1985

Exponential sums over finite fields

Harald Niederreiter*

*Austrian Academy of Sciences

Math. J. Okayama Univ. 27 (1985), 147—158

EXPONENTIAL SUMS OVER FINITE FIELDS

HARALD NIEDERREITER

Let $\mathbf{F}_q$ be the finite field of order q. For $f \in \mathbf{F}_q[x_1, \cdots, x_r]$ and a nontrivial additive character χ of $\mathbf{F}_q$ define the *character sum*

$$C_1 = \sum_{a_1, \cdots, a_r \in \mathbf{F}_q} \chi(f(a_1, \cdots, a_r)).$$

Together with C_1 we consider *lifted character sums* corresponding to the various finite extensions $\mathbf{F}_{q^s}$ of $\mathbf{F}_q$ contained in a fixed algebraic closure $\overline{\mathbf{F}}_q$ of $\mathbf{F}_q$. First, χ is lifted via the trace to a nontrivial additive character $\chi^{(s)}$ of $\mathbf{F}_{q^s}$; in detail, if Tr_s denotes the trace function from $\mathbf{F}_{q^s}$ onto $\mathbf{F}_q$, then set

(1) $$\chi^{(s)}(a) = \chi(\mathrm{Tr}_s(a)) \text{ for } a \in \mathbf{F}_{q^s}.$$

Now define

$$C_s = \sum_{a_1, \cdots, a_r \in \mathbf{F}_{q^s}} \chi^{(s)}(f(a_1, \cdots, a_r)).$$

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) $$L(z) = P(z)^{(-1)^{r-1}}$$

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 $\deg(f)$ is not a multiple of the characteristic of $\mathbf{F}_q$ and the leading homogeneous part f_0 of f is nonsingular in the standard sense (i.e., there is no point over $\overline{\mathbf{F}}_q$ 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 $\deg(f)$ is less than the characteristic of $\mathbf{F}_q$ (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 $L(z)^{-1}$) :

$$(3)\quad L(z) = \exp\left(\sum_{s=1}^{\infty} \frac{C_s}{s} z^s\right) = \prod_{s=1}^{\infty} \exp\left(\frac{C_s}{s} z^s\right) = \prod_{j=1}^{\infty} \left(\sum_{i_j=0}^{\infty} \frac{1}{i_j!} \cdot \frac{C_j^{i_j}}{j^{i_j}} z^{j i_j}\right)$$
$$= 1 + \sum_{s=1}^{\infty} \left(\sum_{i_1+2i_2+\cdots+si_s=s} \frac{C_1^{i_1}\cdots C_s^{i_s}}{i_1!\cdots i_s!\, 2^{i_2}\cdots s^{i_s}}\right) z^s =: 1 + \sum_{s=1}^{\infty} \sigma_s z^s.$$

Now one has to show $\sigma_s = 0$ 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 σ_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 ψ be a multiplicative and χ an additive character of $\mathbf{F}_q$, not both being trivial, and use the convention $\psi(0) = 0$. The corresponding *Gaussian sum* is defined by

$$G_1 = G(\psi, \chi) = \sum_{a \in \mathbf{F}_q} \psi(a)\chi(a).$$

The character ψ is lifted by means of the formula

$$\psi^{(s)}(a) = \psi(\mathrm{N}_s(a)) \text{ for } a \in \mathbf{F}_{q^s},$$

where N_s is the norm function from $\mathbf{F}_{q^s}$ onto $\mathbf{F}_q$. With $\chi^{(s)}$ being given by (1), we consider the *lifted Gaussian sum*

$$G_s = G(\psi^{(s)}, \chi^{(s)}) = \sum_{a \in \mathbf{F}_{q^s}} \psi^{(s)}(a)\chi^{(s)}(a).$$

The Davenport-Hasse theorem expresses the following simple relation between G_s and G_1.

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 $\mathbf{F}_q$. 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

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

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

$$(a_1^{(1)},\cdots,a_{i_1}^{(1)},\cdots,a_1^{(s)},\cdots,a_{i_s}^{(s)}),$$

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

$$t(x) = x^s - t_1x^{s-1} + t_2x^{s-2} \mp \cdots + (-1)^s t_s$$

is irreducible over $\mathbf{F}_q$, 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 $\mathbf{F}_q$. 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 $\mathbf{F}_q$, 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 $M = \{g \in \mathbb{F}_q[x] : g \text{ monic}\}$, $M_r = \{g \in M : \deg(g) = r\}$, $I = \{g \in M : g \text{ irreducible over } \mathbb{F}_q\}$, $I_d = \{g \in I : \deg(g) = d\}$. Define $\lambda : M \to \mathbb{C}$ by $\lambda(1) = 1$ and

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

Then λ 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 $a \in \mathbb{F}_{q^s}$ over $\mathbb{F}_q$, writing g_a for the minimal polynomial of a over $\mathbb{F}_q$, and using simple properties of Tr_s and N_s (see [5, Ch. 2]), we get for $|z| < q^{-1}$:

$$\begin{aligned}
\sum_{s=1}^{\infty} \frac{G_s}{s} z^s &= \sum_{s=1}^{\infty} \frac{z^s}{s} \sum_{d \mid s} \sum_{\deg(a)=d} (\psi^{(d)}(a)\chi^{(d)}(a))^{s/d} \\
&= \sum_{s=1}^{\infty} \frac{z^s}{s} \sum_{d \mid s} \sum_{\deg(a)=d} \lambda(g_a)^{s/d} \\
&= \sum_{s=1}^{\infty} \frac{z^s}{s} \sum_{d \mid s} d \sum_{g \in I_d} \lambda(g)^{s/d} \\
&= \sum_{d=1}^{\infty} \sum_{g \in I_d} \sum_{s=1}^{\infty} \frac{1}{s} (\lambda(g) z^d)^s \\
&= \sum_{d=1}^{\infty} \sum_{g \in I_d} \log \frac{1}{1 - \lambda(g) z^d} \\
&= \log \prod_{g \in I} \frac{1}{1 - \lambda(g) z^{\deg(g)}}.
\end{aligned}$$

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

$$\begin{aligned}
\sum_{s=1}^{\infty} \frac{G_s}{s} z^s &= \log\Big(\sum_{g \in M} \lambda(g) z^{\deg(g)}\Big) = \log\Big(\sum_{r=0}^{\infty}\Big(\sum_{g \in M_r} \lambda(g)\Big) z^r\Big) \\
&= \log(1 + G_1 z) = \sum_{s=1}^{\infty} \frac{1}{s} (-1)^{s-1} G_1^s z^s,
\end{aligned}$$

and comparison of coefficients yields the Davenport-Hasse theorem.

The same method can be applied to other exponential sums. For instance, if ψ_1 and ψ_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*

$$J_s = \sum_{a \in \mathbb{F}_{q^s}} \psi_1^{(s)}(a) \psi_2^{(s)}(b - a).$$

With

$$\lambda(g) = \psi_1((-1)^{\deg(g)}g(0))\psi_2(g(b)) \text{ for } g \in M$$

we get then as above :

$$\sum_{s=1}^{\infty} \frac{J_s}{s} z^s = \log\left(\sum_{r=0}^{\infty}\left(\sum_{g\in M_r} \lambda(g)\right)z^r\right)$$
$$= \log(1+J_1 z) = \sum_{s=1}^{\infty} \frac{1}{s}(-1)^{s-1}J_1^s z^s,$$

and comparison of coefficients yields $J_s = (-1)^{s-1}J_1^s$, 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 χ_i be a nontrivial additive character of F_i, and let ψ_i be an arbitrary multiplicative character of F_i. Let H_1 be a subgroup of the direct product $F_1^* \times \cdots \times F_r^*$ of index m, where F^* 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

$$\overline{\mathrm{N}}_s : F_{1,s}^* \times \cdots \times F_{r,s}^* \to F_1^* \times \cdots \times F_r^*$$

be the componentwise norm function and set $H_s = \overline{\mathrm{N}}_s^{-1}(H_1)$. For fixed $u \in F_1^* \times \cdots \times F_r^*$ define

$$E_s = m \sum_{(a_1,\cdots,a_r)\in uH_s} \chi_1^{(s)}(a_1)\cdots\chi_r^{(s)}(a_r)\psi_1^{(s)}(a_1)\cdots\psi_r^{(s)}(a_r). \tag{4}$$

Then set up the corresponding *L-function*

$$L(z) = \exp\left(\sum_{s=1}^{\infty} \frac{E_s}{s} z^s\right). \tag{5}$$

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

$$L(z) = P(z)^{(-1)^{r-1}}$$

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

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

$$E_s = m \sum_{(a_1,\cdots,a_r)\in H_s} \chi_1^{(s)}(u_1a_1)\cdots\chi_r^{(s)}(u_ra_r)\psi_1^{(s)}(u_1a_1)\cdots\psi_r^{(s)}(u_ra_r). \tag{6}$$

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

$$\text{(7)} \qquad \chi_i^{(s)}(c) = \frac{1}{q_i^s - 1} \sum_{\lambda_i} G(\bar{\lambda}_i, \chi_i^{(s)}) \lambda_i(c) \text{ for all } c \in F_{i,s}^*,$$

where q_i denotes the order of F_i, the Fourier coefficients are Gaussian sums, and $\bar{\lambda}_i$ is the conjugate character of λ_i. Inserting (7) in (6) we get

$$E_s = \frac{m}{(q_1^s-1)\cdots(q_r^s-1)} \sum_{(a_1,\dots,a_r)\in H_s} \psi_1^{(s)}(u_1a_1)\cdots\psi_r^{(s)}(u_ra_r) \cdot \sum_{\lambda_1,\dots,\lambda_r} G(\bar{\lambda}_1, \chi_1^{(s)})\cdots G(\bar{\lambda}_r, \chi_r^{(s)}) \lambda_1(u_1a_1)\cdots\lambda_r(u_ra_r)$$
$$= \frac{m}{(q_1^s-1)\cdots(q_r^s-1)} \sum_{\lambda_1,\dots,\lambda_r} G(\bar{\lambda}_1, \chi_1^{(s)})\cdots G(\bar{\lambda}_r, \chi_r^{(s)})(\psi_1^{(s)}\lambda_1)(u_1)\cdots (\psi_r^{(s)}\lambda_r)(u_r) \sum_{(a_1,\dots,a_r)\in H_s} (\psi_1^{(s)}\lambda_1)(a_1)\cdots(\psi_r^{(s)}\lambda_r)(a_r).$$

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 $(\psi_1^{(s)}\lambda_1, \cdots, \psi_r^{(s)}\lambda_r) \in A_s$ and 0 otherwise. Therefore,

$$\text{(8)} \qquad E_s = \frac{m|H_s|}{(q_1^s-1)\cdots(q_r^s-1)} \sum_{(\lambda_1,\dots,\lambda_r)\in A_s} G(\bar{\lambda}_1\psi_1^{(s)}, \chi_1^{(s)})\cdots G(\bar{\lambda}_r\psi_r^{(s)}, \chi_r^{(s)}) \lambda_1(u_1)\cdots\lambda_r(u_r).$$

Since $\bar{N}_s$ is surjective, we have

$$|\ker \bar{N}_s| = \frac{(q_1^s-1)\cdots(q_r^s-1)}{(q_1-1)\cdots(q_r-1)},$$

and from $H_1 \simeq H_s/\ker \bar{N}_s$ we get

$$\text{(9)} \qquad |H_s| = |H_1| \frac{(q_1^s-1)\cdots(q_r^s-1)}{(q_1-1)\cdots(q_r-1)}.$$

This implies

$$\text{(10)} \qquad |A_s| = \frac{(q_1^s-1)\cdots(q_r^s-1)}{|H_s|} = \frac{(q_1-1)\cdots(q_r-1)}{|H_1|} = |A_1|.$$

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

$$E_s = \sum_{(\lambda_1,\ldots,\lambda_r)\in A_1} G(\bar{\lambda}_1^{(s)}\psi_1^{(s)}, \chi_1^{(s)})\cdots G(\bar{\lambda}_r^{(s)}\psi_r^{(s)}, \chi_r^{(s)})\lambda_1^{(s)}(u_1)\cdots\lambda_r^{(s)}(u_r).$$

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

$$E_s = (-1)^r \sum_{(\lambda_1,\ldots,\lambda_r)\in A_1} ((-1)^r G(\bar{\lambda}_1\psi_1, \chi_1)\cdots G(\bar{\lambda}_r\psi_r, \chi_r)\lambda_1(u_1)\cdots\lambda_r(u_r))^s.$$

Since $|A_1| = m$, we can label the numbers

(11) $$(-1)^r G(\bar{\lambda}_1\psi_1, \chi_1)\cdots G(\bar{\lambda}_r\psi_r, \chi_r)\lambda_1(u_1)\cdots\lambda_r(u_r)$$

by $\omega_1,\cdots,\omega_m$, so that

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

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

$$L(z) = \exp\left((-1)^r \sum_{s=1}^{\infty} \frac{z^s}{s} \sum_{j=1}^{m} \omega_j^s\right) = \exp\left((-1)^r \sum_{j=1}^{m}\sum_{s=1}^{\infty} \frac{1}{s}(\omega_j z)^s\right)$$
$$= \exp\left((-1)^{r-1} \sum_{j=1}^{m} \log(1-\omega_j z)\right) = P(z)^{(-1)^{r-1}}$$

with

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

Since the characters χ_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), $n = 0, 1, \cdots$, be a *linear recurring sequence* in $\mathbf{F}_q$ satisfying the linear recurrence relation

(13) $$y_{n+k} = b_{k-1}y_{n+k-1}+\cdots+b_0 y_n, \quad n = 0, 1, \cdots,$$

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

$$f(x) = x^k - b_{k-1}x^{k-1} - \cdots - b_0 \in \mathbf{F}_q[x]$$

is the *minimal polynomial* of (y_n) (compare with [5, Ch. 8]). Then the least period τ 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 v_i be a fixed root of f_i in its splitting field F_i over K, and let $\mathrm{Tr}_{F_i/K}$ 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*

$$y_n = \sum_{i=1}^{r} \mathrm{Tr}_{F_i/K}(u_i v_i^n) \text{ for } n = 0, 1, \cdots.$$

Proof. Let

$$G(x) = \sum_{n=0}^{\infty} y_n x^n \tag{14}$$

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, Ch. 8]). By partial fraction decomposition,

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

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

$$\begin{aligned} G(x) &= \sum_{i=1}^{r} \sum_{j=0}^{d_i-1} a_{ij} \sum_{n=0}^{\infty} v_i^{nq^j} x^n = \sum_{n=0}^{\infty} \left(\sum_{i=1}^{r} \sum_{j=0}^{d_i-1} (a_{i0} v_i^n)^{q^j} \right) x^n \\ &= \sum_{n=0}^{\infty} \left(\sum_{i=1}^{r} \mathrm{Tr}_{F_i/K}(a_{i0} v_i^n) \right) x^n, \end{aligned}$$

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 χ be a nontrivial additive character of $K = \mathbf{F}_q$ and consider the character sum

$$\sum_{n=0}^{\tau-1} \chi(y_n) \tag{15}$$

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

$$\begin{aligned}\sum_{n=0}^{\tau-1} \chi(y_n) &= \sum_{n=0}^{\tau-1} \chi(\mathrm{Tr}_{F_1/K}(u_1 v_1^n))\cdots\chi(\mathrm{Tr}_{F_r/K}(u_r v_r^n)) \\ &= \sum_{n=0}^{\tau-1} \chi^{(d_1)}(u_1 v_1^n)\cdots\chi^{(d_r)}(u_r v_r^n) \\ &= \sum_{(a_1,\dots,a_r)\in uH_1} \chi^{(d_1)}(a_1)\cdots\chi^{(d_r)}(a_r),\end{aligned}$$

where $u = (u_1, \cdots, u_r) \in F_1^* \times \cdots \times F_r^*$ and H_1 is the cyclic subgroup of $F_1^* \times \cdots \times F_r^*$ generated by $(v_1, \cdots, v_r)$. 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 ψ_i for $1 \leq i \leq r$.

The identity (12), together with the form of the ω_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 $F_i = \mathbf{F}_q$ 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*

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

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

$$|E_s| \geq (C-\varepsilon)q^{sH/2}.$$

Proof. By (12) we have

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

where the ω_j are given by (11). For $0 \leq h \leq r$ let m_h be the number of

$(\lambda_1,\cdots,\lambda_r)\in A_1$ such that $\lambda_i=\psi_i$ holds for exactly h values of i. Then

(16) $$\sum_{h=0}^{r} m_h = m.$$

We note the fact that for a multiplicative character ψ and a nontrivial additive character χ 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) $$|E_s| \leq \sum_{h=0}^{r} m_h q^{s(r-h)/2}.$$

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

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

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 $|\omega_j|=q^{H/2}$. For $j\in J$ we have

$$\omega_j = q^{H/2}e^{2\pi i\theta_j} \text{ with } \theta_j \text{ real}.$$

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,

$$\begin{aligned}|E_s| &\geq \left|\sum_{j\in J}\omega_j^s\right| - \left|\sum_{j\notin J}\omega_j^s\right| = q^{sH/2}\left|\sum_{j\in J}e^{2\pi i s\theta_j}\right| - \left|\sum_{j\notin J}\omega_j^s\right| \\ &\geq \left(C-\frac{\varepsilon}{2}\right)q^{sH/2}-(m-C)q^{s(H-1)/2} \geq (C-\varepsilon)q^{sH/2}\end{aligned}$$

for infinitely many s.

An interesting special case for applications is that of the character sums in (15), with the minimal polynomial f of (y_n) being irreducible over $\mathbb{F}_q$. In this case $r=1$, $F_1=\mathbb{F}_{q^k}$, and H_1 is the subgroup of F_1^* generated by a root ν 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 ψ_1 trivial. The lifted sum E_s, $s \geq 2$, corresponds to a subgroup H_s of $F_{1,s}^*$ of the same index m. Now H_s is cyclic of order $\tau_s = (q^{ks} - 1)/m$, so we can choose a generator $\nu^{(s)}$ of H_s. Let $f^{(s)}$ be the minimal polynomial of $\nu^{(s)}$ over $\mathbb{F}_{q^s}$. It is clear that $d = \deg(f^{(s)})$ divides k. Suppose d were a proper divisor of k. Then it follows that

$$\tau_s = \frac{(q^{ks} - 1)\tau}{q^k - 1} = (q^{k(s-1)} + q^{k(s-2)} + \cdots + 1)\tau > q^{ks/2} > q^{sd} - 1.$$

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

$$(\nu^{(s)})^{q^{sd}-1} = 1,$$

which implies $\tau_s \leq q^{sd} - 1$, 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 τ_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*

$$\left| \sum_{n=0}^{\tau_s-1} \chi^{(s)}(y_n^{(s)}) \right| \leq \left(1 - \frac{\tau_s}{q^{ks} - 1}\right) q^{ks/2} + \frac{\tau_s}{q^{ks} - 1}. \tag{18}$$

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

Mathematical Journal of Okayama University, Vol. 27 [1985], Iss. 1, Art. 21

$$\sum_{n=0}^{\tau_S-1} \chi^{(S)}(y_n^{(S)}) = -1,$$

and so (18) is again best possible.

References

[1] E. Bombieri: On exponential sums in finite fields, Amer. J. Math. 88 (1966), 71–105.

[2] H. Davenport and H. Hasse: Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen, J. reine angew. Math. 172 (1935), 151–182.

[3] P. Deligne: La conjecture de Weil. I, Inst. Hautes Etudes Sci. Publ. Math. 43 (1974), 273–307.

[4] A. Grothendieck: Formule de Lefschetz et rationalité des fonctions L, Sém. Bourbaki 1964/65, Exp. 279, Benjamin, New York, 1966.

[5] R. Lidl and H. Niederreiter: Finite Fields, Encyclopedia of Math. and Its Appl., vol. 20, Addison-Wesley, Reading, Mass., 1983.

[6] H. H. Mitchell: On the generalized Jacobi-Kummer cyclotomic function, Trans. Amer. Math. Soc. 17 (1916), 165–177.

[7] H. Niederreiter: Some new exponential sums with applications to pseudo-random numbers, Topics in Number Theory (Debrecen, 1974), Colloquia Math. Soc. János Bolyai, vol. 13, pp. 209–232, North-Holland, Amsterdam, 1976.

[8] H. Niederreiter: On the cycle structure of linear recurring sequences, Math. Scand. 38 (1976), 53–77.

[9] H. Niederreiter: Quasi-Monte Carlo methods and pseudo-random numbers, Bull. Amer. Math. Soc. 84 (1978), 957–1041.

[10] H. L. Schmid: Relationen zwischen verallgemeinerten Gaußschen Summen, J. reine angew. Math. 176 (1937), 189–191.

[11] S. A. Stepanov: Proof of the Davenport-Hasse relations (Russian), Mat. Zametki 27 (1980), 3–6.

[12] S. A. Stepanov: Exponential sums in several variables and L-functions of Artin, Tagungsbericht Analytische Zahlentheorie, Math. Forschungsinst. Oberwolfach, 1982.

[13] S. A. Stepanov: Rational trigonometric sums and Artin L-functions (Russian), Dokl. Akad. Nauk SSSR 265 (1982), 39–42.

[14] L. Stickelberger: Ueber eine Verallgemeinerung der Kreistheilung, Math. Ann. 37 (1890), 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.