PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 111, Number 2, February 1991

EXPONENTIAL SUMS AND GOPPA CODES: I

CARLOS J. MORENO AND OSCAR MORENO

(Communicated by Andrew Odlyzko)

ABSTRACT. A bound is obtained which generalizes the Carlitz–Uchiyama result, based on a theorem of Bombieri and Weil about exponential sums. This new bound is used to estimate the covering radius of long binary Goppa codes. A new lower bound is also derived on the minimum distance of the dual of a binary Goppa code, similar to that for BCH codes. This is an example of the use of a number-theory bound for the problem of the estimation of minimum distance of codes, as posed in research problem 9.9 of MacWilliams and Sloane, *The Theory of Error Correcting Codes.*

1. INTRODUCTION

We will consider the Goppa code $\Gamma(L, G)$ with Goppa polynomial $G(x)$ of degree t with coefficients in $\mathbf{F} = \mathbf{F}_{2^m}$, the finite field of 2^m elements, and $L = \mathbf{F} - Z$, where Z is the set of zeros of $G(x)$ in F. We assume that $G(x)$ satisfies the following condition:

(A) The polynomial $G(x)$ has distinct roots.

In the past, bounds for exponential sums of the Carlitz–Uchiyama type have been used by Helleseth [4] and Tietavainen [7] to obtain bounds for the covering radius of long BCH codes. In this article we derive a generalization of the Carlitz–Uchiyama bound and use it to obtain the following analogue of the Helleseth bound for Goppa codes:

Theorem 1. *Let $c = c(L, G)$ be the covering radius of the Goppa code $\Gamma(L, G)$, with G and L as above. We have*

$$c \leq 2t + 1,$$

Received by the editors August 16, 1988 and, in revised form, November 27, 1989; the contents of this paper were presented at the International Workshop on Algebraic and Combinatorial Coding Theory, Varma, Bulgaria, September 18–24, 1988.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 94B05, 14G10.

The first author's work was partially supported by grant DMS-8711566 from the National Science Foundation.

The second author's work was partially supported by NSF grants DCI-86011555 and RII-8604333 and component IV of the EPSCOR of Puerto Rico Proposal.

whenever

$$q > \left(\frac{2\deg G - 2}{1 - zq^{-1}}\right)^{4t+2},$$

and where $z = \mathrm{Card}(Z)$.

Remark. Observe that, when $L = F$, the bound above holds when

$$q > (2\deg G - 2)^{4t+2},$$

which is remarkably similar to the Helleseth bound for BCH codes.

The proof of this result is based on the following theorem, in the case where the characteristic is 2. The theorem estimates exponential sums and is of independent interest. Let $R(x) = F(x)/G(x)$ be a rational function in $\mathscr{F}(x)$ which satisfies the condition

(B) $R(x) \neq h(x)^p - h(x)$ for any $h \in \overline{\mathbf{F}}(x)$, $\overline{\mathbf{F}}$ the algebraic closure of $\mathbf{F}$.

Theorem 2. *Let* $\mathbf{F}$ *be the finite field of* q *elements and characteristic* p; *let* $R(x) = F(x)/G(x)$ *be a quotient of two polynomials with coefficients in* $\mathbf{F}$ *that satisfies condition* (B) *above. Let* s *be the number of distinct roots of* $G(x)$ *in* $\overline{\mathbf{F}}$. *If* $\Psi(a)$ *denotes a nontrivial additive character of* $\mathbf{F}$, *then we have*

$$\left|\sum_{x\in L} \Psi(R(x))\right| \leq (\max(\deg F, \deg G) + s^* - 2)q^{1/2} + \delta,$$

where the sum $\sum$ *runs over all* $x \in \mathbf{F}$ *excluding the zeros of* $G(x)$; $s^* = s$ *and* $\delta = 1$ *when* $\deg F \leq \deg G$, *and* $s^* = s + 1$ *and* $\delta = 0$ *otherwise.*

In one of the earliest applications of the Carlitz–Uchiyama bound to coding theory, the minimum distance for $\mathscr{C}^*$, the dual of a binary BCH code $\mathscr{C}$ of length $n = 2^m - 1$ and designed distance $d = 2t + 1$, was estimated to be at least $2^{m-1} - (t-1)2^{m/2}$ [5, Corollary 20, p. 281]. In this paper we also prove the following remarkable similar result for binary Goppa codes.

Theorem 3. *The minimum distance of* $\Gamma(L, G)^*$, *the dual of* $\Gamma(L, G)$, *is at least* $2^{m-1} - (\frac{k-1}{2}) - (t-1)2^{m/2}$, *where* k *is the number of zeros of* $G(x)$ *in* $\mathbf{F}$.

We also obtain the following corollary.

Corollary 1. *If* $G(x)$ *has no zeros in* $\mathbf{F}$, *then the minimum distance of* $\Gamma(L, G)^*$ *is at least* $2^{m-1} + \frac{1}{2} - (t-1)2^{m/2}$.

This last estimate gives a slightly better minimum distance than the bound $2^{m-1} - (t-1)2^{m/2}$ that one can obtain for BCH codes [5, p. 281].

The proof of Theorem 1 is given in §2 using the method first used by Helleseth in [4] (see also [7]) and that of Theorem 2 is given in §3 from the general estimate of Bombieri–Weil [1, 2]. Theorem 3 is proved in §4 using our estimates for exponential sums and some well-known results of Delsarte. In an appendix, we include a precise statement of the theorem of Bombieri–Weil.

2. Proof of Theorem 1

Throughout this section we assume that $\mathbf{F} = \mathbf{F}_{2^m}$ is the finite field of $q = 2^m$ elements. Using the notation of the introduction and of [5], we recall that the parity matrix of the Goppa code $\Gamma(L, G)$ with $l = \{\alpha_1, \dots, \alpha_n\} = \mathbf{F} - Z$ is

$$H = \begin{pmatrix} \frac{1}{G(\alpha_1)} & \cdots & \frac{1}{G(\alpha_n)} \\ \frac{\alpha_1}{G(\alpha_1)} & \cdots & \frac{\alpha_n}{G(\alpha_n)} \\ \vdots & & \vdots \\ \frac{\alpha_1^{t-1}}{G(\alpha_1)} & \cdots & \frac{\alpha_n^{t-1}}{G(\alpha_n)} \end{pmatrix},$$

where $t = \deg G$. As in [4], it is easy to see that the covering radius r is the smallest positive integer such that given arbitrary elements $b_1, \dots, b_t \in \mathbf{F}$, there is a solution to the system

$$(*)\qquad \begin{aligned} \frac{1}{G(x_1)} + \cdots + \frac{1}{G(x_r)} &= b_1 \\ \frac{x_1}{G(x_1)} + \cdots + \frac{x_r}{G(x_r)} &= b_2 \\ &\cdots \\ \frac{x_1^{t-1}}{G(x_1)} + \cdots + \frac{x_r^{t-1}}{G(x_r)} &= b_t. \end{aligned}$$

If Ψ is a nontrivial character of $\mathbf{F}$, then recall that the orthogonality relations state that

$$\sum_{x \in F} \Psi(\alpha x) = q\delta_{\alpha,0},$$

where $\delta_{\alpha,\beta}$ is the Kronecker delta. For ease of notation, let us assume that G does not have zeros in $\mathbf{F}$; that is, $\mathbf{F} = L$. Now, if N_r denotes the number of r tuples $\underline{x} = (x_1, \dots, x_r)$ in $P(F)^r$ that are solutions of the system $(*)$, then

$$\begin{aligned} q^t N_r = \sum_{\underline{x} \in P(F)^r} & \left(\sum_{\alpha_1 \in F} \Psi\left(\alpha_1 \left(\frac{1}{G(x_1)} + \cdots + \frac{1}{G(x_r)} + b_1\right)\right)\right) \\ & \times \cdots \times \left(\sum_{\alpha_t \in F} \Psi\left(\alpha_t \left(\frac{x_1^{t-1}}{G(x_1)} + \cdots + \frac{x_r^{t-1}}{G(x_r)} + b_t\right)\right)\right) \\ = \sum_{(\alpha_1, \dots, \alpha_t) \in F^t} & \Psi(\alpha_1 b_1 + \cdots + \alpha_t b_t) \\ & \times \left(\sum_{x_1 \in P(F)} \Psi\left(\frac{\alpha_1}{G(x_1)} + \frac{\alpha_2 x_1}{G(x_1)} + \cdots + \frac{\alpha_t x_1^{t-1}}{G(x_1)}\right)\right) \\ & \times \cdots \times \left(\sum_{x_r \in P(F)} \Psi\left(\frac{\alpha_1}{G(x_r)} + \frac{\alpha_2 x_r}{G(x_r)} + \cdots + \frac{\alpha_r x_r^{t-1}}{G(x_r)}\right)\right). \end{aligned}$$

(Observe that if $x_1, \dots, x_{r-1}$ is a solution of the above system, then P_∞, $x_1, \dots, x_{r-1}$ is also a solution. Also note that, if we add over $P(\mathbf{F})$, then we may apply the full strength of Bombieri's theorem as stated in Corollary 3.) If $\alpha_1 = \cdots = \alpha_t = 0$, then the above sum gives a contribution of q and

$$q^t N_r - q^r = \sum_{(\alpha_1, \dots, \alpha_t)} \Psi(\alpha_1 b_1 + \cdots + \alpha_t b_t) \left(\sum_{x \in P(F)} \Psi\left(\frac{\alpha_1}{G(x)} + \cdots + \frac{\alpha_t x^{t-1}}{G(x)} \right) \right)^r .$$

Now we suppose that the Goppa polynomial $G(x)$ satisfies condition (A), necessary for the validity of Lemma 1 below, which will permit us to invoke Theorem 2. Let

$$F(x) = \alpha_1 + \alpha_2 x + \cdots + \alpha_t x^{t-1}$$

be an arbitrary polynomial in $F[x]$ so that Theorem 2 yields the estimate:

$$\left| \sum_{x \in P(F)} \Psi\left(\frac{F(x)}{G(x)} \right) \right| \le (2 \deg G - 2) q^{1/2}.$$

The last inequality yields

$$|q^t N_r - q^r| \le (q^t - 1)[(2 \deg G - 2) q^{1/2}]^r.$$

If $N_r = 0$, then

$$q^r \le (q^t - 1)[a q^{1/2}]^r,$$

with $a = 2 \deg G - 2$. Recall that $\deg G = t$; hence, $a = 2t - 2$. This implies that

$$q^{r/2} \le (q^t - 1) a^r < q^t a^r;$$

hence, if the number of variables r is $2t + 1$, and q is chosen so that

$$q \ge a^{2r},$$

it follows that $N_r \ne 0$; i.e., the system $(*)$ has nontrivial solutions. In particular, when the inequality $q \ge a^{4t+2}$ is satisfied, the covering radius of the Goppa code $\Gamma(L, G)$ is $\le 2t + 1$.

To obtain the claim in Theorem 1, we must exclude the zeros of $G(x)$ from the sum. The resulting inequality is

$$|q^t N_r - \operatorname{Card}(L)^r| \le (q^t - 1)((2 \deg G - 2) q^{1/2})^r,$$

and since $\operatorname{Card}(L) = q - z$, the system has solutions for

$$q > \left(\frac{2 \deg G - 2}{1 - z q^{-1}} \right)^{4t+2},$$

and the covering radius is $\le 2t + 1$.

Lemma 1. *Let $f(x)$, $G(x) \in F_{2^m}[x]$ be such that $G(x)$ has distinct roots. Then, for an arbitrary extension F' of F, we cannot find $\alpha(x)$, $\beta(x) \in F'[x]$ such that*

$$\frac{f(x)}{G(x)} = \left(\frac{\alpha(x)}{\beta(x)}\right)^2 + \frac{\alpha(x)}{\beta(x)} + \gamma.$$

Proof. Assume that $\alpha(x)$ and $\beta(x)$ do exist and, without loss of generality, suppose further that $(\alpha(x), \beta(x)) = 1$. Then we have

$$\frac{f(x)}{G(x)} = \frac{(\alpha^2(x) + \alpha(x)\beta(x) + \gamma\beta^2(x))}{\beta^2(x)}.$$

The right-hand side cannot be simplified; there is no factor of $\beta(x)$ that is also a factor of the numerator $\alpha^2(x) + \alpha(x)\beta(x) + \gamma\beta^2(x)$. If this was not the case, we would contradict $(\alpha(x), \beta(x)) = 1$. Now we can conclude from the above equality that $\beta^2(x)$ divides $G(x)$, and this contradicts our assumption on the distinctness of the roots of $G(x)$.

3. A GENERALIZED CARLITZ–UCHIYAMA BOUND

In this section we use Theorem 3 of the appendix to derive our generalization of the Carlitz–Uchiyama bound given in Theorem 2. Our starting point is the projective line $\mathscr{C}_0 = \mathscr{P}^1$, and the rational function is the quotient $R(x) = F(x)/G(x)$ of two polynomials $F(x)$ and $G(x)$ with coefficients in F. The main auxiliary calculation needed is the degree of the divisor of poles of $R(x)$; here we review the well-known results about points on the projective line $\mathscr{P}^1$ and discrete valuations on $F(x)$ (see [6]).

If we denote by $x_\infty = 1/x$ the local uniformizing parameter for the point at infinity P_∞ on the projective line, then the corresponding valuation

$$v_\infty : F(x) \to Z$$

assigns the value $v_\infty(G) = \deg G$ to the polynomial $G(x)$. The discrete valuations $v_P : F(x) \to Z$ corresponding to the finite points are in one-to-one correspondence with the irreducible polynomials in $F[x]$: with the irreducible polynomial $P(x)$ associated with the valuation v_P, which assigns the value $v_P(R) = e$ whenever

$$R(x) = P(x)^e A(x)/B(x),$$

with $A(x)$, $B(x)$ relatively prime to $P(x)$. If we let

$$F(x) = a\prod_{i=1}^{r} F_i(x)^{d_i}$$

be the unique factorization of $F(x)$ into irreducible polynomials in $F[x]$, then the divisor of $F(x)$ as a rational function on $\mathscr{P}^1$ is

$$(F) = -(\deg G)P_\infty + \sum_{i=1}^{r} d_i P_i,$$

where P_i is the point on $\mathscr{P}^1$ corresponding to the irreducible factor $F_i(x)$. Similarly, if

$$G(x) = b\prod_{j=1}^{u} G_j(x)^{e_j}$$

is the unique factorization of $G(x)$ in $F[x]$, then its divisor as a rational function on $\mathscr{P}^1$ is also

$$(G) = -(\deg G)P_\infty + \sum_{j=1}^{u} e_j Q_j,$$

where Q_j is the point on $\mathscr{P}^1$ corresponding to G_j. Thus we obtain the divisor of the rational function $R(x) = F(x)/G(x)$:

$$(R) = (F) - (G) = (\deg G - \deg F)P_\infty + \sum_{i=1}^{r} d_i P_i - \sum_{j=1}^{u} e_j Q_j.$$

Therefore the divisor of poles of R is

$$(R)_\infty = (\deg F - \deg G)P_\infty + \sum_{j=1}^{u} e_j Q_j \quad \text{if } \deg F > \deg G,$$

and

$$\sum_{j=1}^{u} e_j Q_j \quad \text{if } \deg F \le \deg G.$$

In particular, the degree of $(R)_\infty$ is

$$\deg(R)_\infty = \max(\deg F, \deg G).$$

If we observe that the number of distinct poles of $R(x) = F(x)/G(x)$ over $\overline{F}$ is

$$s^* := s = \sum_{j=1}^{u} \deg G_j \quad \text{if } \deg F \le \deg G$$

(i.e., $R(x)$ is finite at the point at infinity, and $s^* := s+1$, when $\deg F > \deg G$) then using the fact that the genus of the projective line is 0, we obtain from the Bombieri–Weil result (see Theorem 4 of the Appendix), the inequality

$$\left|\sum_{x\in L\cup(P_\infty)} \Psi(R(x))\right| \le (\max(\deg F, \deg G) + s^* - 2)q^{1/2},$$

where the sum $\sum$ is taken over all x in the projective line $\mathscr{P}^1(F) = F \cup (P_\infty)$ excluding the poles of $R(x)$. Now, if we observe that

$$\sum_{x\in L\cup(P_\infty)} \Psi(R(x)) = \sum_{x\in L} \Psi(R(x)) + \delta\Psi(R(P_\infty)),$$

where $\delta = 0$ if P_∞ is a pole of $R(x)$ and $\delta = 1$ otherwise, we obtain

$$\left|\sum \Psi(R(x))\right| \le (\max(\deg F, \deg G) + s^* - 2)q^{1/2} + 1.$$

This establishes Theorem 2. We add the following consequence:

Corollary 1 (Carlitz–Uchiyama [2]). *If* $\deg G = 0$ *and* $R(x) = F(x)$ *is a polynomial in* $F(x)$, *then*

$$\left|\sum_{x\in F}\Psi(F(x))\right| \le (\deg F - 1)q^{1/2}.$$

Corollary 2. *Let* $G(x)$ *have distinct roots, and suppose that* $\deg G > \deg F$. *Then*

$$-(2\deg G-2)q^{1/2}-1 \le \sum_{x\in L}\Psi(R(x)) \le (2\deg G-2)q^{1/2}-1,$$

where $\sum$ *is taken over all* $x\in F$ *excluding the zeros of* $G(x)$.

Note. The sharper inequality in Corollary 2 comes from the fact that P_∞ is actually a zero of $F(x)/G(x)$, and hence its contribution to the sum is $+1$.

Corollary 3. *Let* $G(x)$ *have distinct roots, and suppose that* $\deg G > \deg F$. *Then*

$$-(2\deg G-2)q^{1/2} \le \sum_{x\in L\cup P_\infty}\Psi(R(x)) \le (2\deg G-2)q^{1/2},$$

where $\sum$ *is taken over all* $x\in P(F)$ *excluding the zeros of* $G(x)$.

4. Proof of Theorem 3

We recall the following results from MacWilliams and Sloane [5]. They are originally due to Delsarte [3].

We define the generalized Reed–Solomon code as

$$\mathrm{GRS}_r(\alpha, y) = \{(y_1F(\alpha_1), \dots, y_nF(\alpha_n)) : F(x)\in \mathbf{F}[x], \deg F < r\},$$

where $\alpha = \{\alpha_1, \dots, \alpha_n\}$ is a fixed set of distinct elements in $\mathbf{F}$ and $y = \{y_1, \dots, y_n\}$ is a fixed set of n elements in $\mathbf{F}$.

For $\mathscr{C}$ a code over $\mathbf{F}_{2^m}$, $T_m(\mathscr{C})$ denotes the code over $\mathbf{F}_2$ whose elements are obtained from code words of $\mathscr{C}$ by taking the trace from $\mathbf{F}_{2^m}$ down to $\mathbf{F}_2$ componentwise.

Theorem (MacWilliams and Sloane [5, p. 341]). *The dual of a Goppa code is given by*

$$\Gamma(L, G)^* = T_m(\mathrm{GRS}_t(\alpha, y)),$$

where $y_i = G(\alpha_i^{-1})$ *and* $t = \deg G$.

From the above theorem we have

$$\Gamma(L, G)^* = \left\{\left(T_m\left(\frac{F(\alpha_1)}{G(\alpha_1)}\right), \dots, T_m\left(\frac{F(\alpha_n)}{G(\alpha_n)}\right)\right) : F(x)\in\mathbf{F}[x], \deg F < t\right\}.$$

Consider the additive character $\psi(\theta) = (-1)^{T_m(\theta)}$ defined for θ in $\mathbf{F}$. Now if we consider an arbitrary polynomial F of degree $< t$ then, using Corollary 2 of §3, we obtain

$$\left|1+\sum_{x\in L}\psi\left(\frac{F(x)}{G(x)}\right)\right| \le (2\deg G-2)q^{1/2},$$

and we note that L is precisely $\mathbf{F} - Z$ where Z is the set of zeros of $G(x)$ in $\mathbf{F}$. Now we observe that if $x = (x_1, \ldots, x_n) \in \Gamma(L, G)^*$, then

$$x = \left(T_m\left(\frac{F(\alpha_1)}{G(\alpha_1)}, \ldots, T_m\left(\frac{F(\alpha_n)}{G(\alpha_n)}\right)\right)\right),$$

and hence the weight w of x and the number z of zero components of x have the property $z + w = n$ and

$$\sum_{x \in L} \psi\left(\frac{F(x)}{G(x)}\right) = z - w = n - 2w.$$

Therefore,

$$1 + n + 2w \leq (2t-2)q^{1/2}$$

and

$$w \geq \frac{n+1}{2} - (t-1)q^{1/2}.$$

These inequalities show that the minimum distance is at least

$$2^{m-1} - \left(\frac{k-1}{2}\right) - (t-1)q^{1/2}.$$

This completes the proof of Theorem 3.

5. Appendix

A precise statement of the Bombieri–Weil estimate for exponential sums in one variable and the associated Artin–Schreier coverings is given here.

Let $\mathscr{C}_0$ be a complete nonsingular curve of genus g defined over F so that its field of functions $F(\mathscr{C}_0)$ can be realized as an algebraic extension of the pure transcendental extension $F(x)$ with exact field of constants F. Let $\overline{F}(\mathscr{C}_0)$ be the function field of $\mathscr{C}_0$ considered over the algebraic closure $\overline{F}$ of F. Let $R(x)$ be a rational function satisfying the condition

$$\text{(B)} \qquad R(x) \neq h(x)^p - h(x) \quad \text{for } h(x) \in \overline{F}(\mathscr{C}_0).$$

If P is a point on the curve $\mathscr{C}_0$, we denote by $R(P)$ the value of $R(x)$ at P; this is an element of the residue class field $F_P = F_P(\mathscr{C}_0)$. Let $\mathscr{C}_0(F_m)$ be the rational points of $\mathscr{C}_0$ defined over the extension F_m of F of degree m, and let $\sigma\colon F_P \to F$ be the relative trace from F_P to F. We define the exponential sum

$$\Psi_m(R, \mathscr{C}_0) = \sum_{P \in \mathscr{C}_0(F_m) - \{\text{poles}\}} \Psi(\sigma R(P)),$$

where the sum $\sum$ is restricted to those points P in $\mathscr{C}_0(F_m)$ that are not poles of $R(x)$. This type of exponential sum is related to the zeta function of a certain Artin–Schreier covering of $\mathscr{C}_0$ that we now describe in greater detail.

Let $\mathscr{C}'$ be the curve defined by the equation

$$\mathscr{C}' : y^p - y = R(x).$$

This is a Galois covering $\pi: \mathscr{C}' \to \mathscr{C}_0$, with Galois group $\mathbf{Z}/p\mathbf{Z}$ acting on $\mathscr{C}'$ by means of the substitution $y \mapsto y + g$. If $\mathscr{C}$ denotes the normalization of $\mathscr{C}'$, then the map $\mathscr{C} \to \mathscr{C}'$ gives the Artin–Schreier covering

$$\pi: \mathscr{C} \rightharpoonup \mathscr{C}_0$$

associated with the rational function $R(x)$. In the following, we let $(R)_\infty$ be the divisor of poles of $R(x)$ on $\mathscr{C}_0$ and write

$$(R)_\infty = \sum_{i=1}^{t} d_i P_i,$$

where the P_i are points on $\mathscr{C}_0$ and the d_i are the multiplicity of the pole of $R(x)$ at P_i. The following is essentially the result of Bombieri–Weil:

Theorem 4 [1, p. 94]. *With notation as above, we have*

$$|\Psi_m(R, \mathscr{C}_0)| \le (2g - 2 + t + \deg(R)_\infty) q^{m/2}.$$

Moreover, the above inequality cannot be improved if $(d_i, p) = 1$ *for all* $i = 1, \ldots, t$.

Acknowledgment

The first author wishes to thank the Gauss Center for Computational Research of the University of Puerto Rico for its hospitality during the execution of this work. The second author wishes to thank City University of New York for its hospitality.

References

1. E. Bombieri, *On exponential sums in finite fields*, Amer. J. Math. **88** (1966), 71–105.
2. L. Carlitz and S. Uchiyama, *Bounds for exponential sums*, Duke Math. J. **24** (1957), 37–41.
3. P. Delsarte, *On subfield subcodes of Reed-Solomon codes*, IEEE Trans. Info. Theory **21** (1975), 575–576.
4. T. Helleseth, *On the covering radius of cyclic linear codes and arithmetic codes*, Discrete Appl. Math. **11** (1985), 157–173.
5. F. J. MacWilliams and N. J. A. Sloane, *The theory of error correcting codes*, North-Holland, Amsterdam, 1977.
6. C. J. Moreno, *Algebraic curves over finite fields and error correcting codes*, Cambridge Univ. Press (to appear).
7. A. Tietavainen, *On the covering radius of long binary BCH codes*, Discrete Applied Math. **16** (1987), 75–77.
8. A. Weil, *On some exponential sums*, Proc. Natl. Acad. Sci. USA **34** (1948), 204–207.

Department of Mathematics, City University of New York, New York, New York 10010

Department of Mathematics, University of Puerto Rico, Rio Piedras, Puerto Rico 00931