

On relations between certain exponential sums and multiple Kloosterman sums and some applications to coding theory

MARKO MOISIO

Abstract. In this paper we consider some relations between multiple Kloosterman sums and certain exponential sums with monomial and binomial arguments, and some applications of these relations to coding theory.

1. Introduction

Let $F = \mathbb{F}_q$ denote the finite field with q elements and $E = \mathbb{F}_{q^m}$ be an extension of degree $m > 1$ of F . In this paper we consider relations between certain exponential sums

$$S(f) := \sum_{x \in E} e_E(f(x)),$$

and (multiple) Kloosterman sums

$$K_m(a) := \sum_{x_1, \dots, x_m \in F^*} e_F(x_1 + \dots + x_m + ax_1^{-1} \dots x_m^{-1}),$$

where e_E (resp. e_F) is the canonical additive character of E (resp. F), $f(X) \in E[X]$, $a \in F$, $\gcd(q, \deg f(X)) = 1$, and some applications of these relations to coding theory.

More precisely, we shall construct a class of binary irreducible cyclic codes and two classes of binary cyclic codes (by means of certain well known irreducible cyclic

codes), and estimate the weights of the words of these codes by using the Weil and the Deligne bounds, obtained by Weil in [12] and by Deligne in [1]:

$$|S(f)| \leq (\deg f(X) - 1)q^{m/2}, \quad (1)$$

$$|K_m(a)| \leq (m + 1)q^{m/2}. \quad (2)$$

It turns out e.g. that the weight distribution of the binary cyclic code constructed by means of two simplex codes of different length is closely related to the values of a multiple Kloosterman sum over a field of characteristic 2.

2. On relations between certain exponential sums and multiple Kloosterman sums

We assume that F , E , e_F , e_E and $K_m()$ are fixed as in the introduction. We also denote the canonical additive character of E (resp. F) simply by e if this does not cause any confusions.

Let $\text{Tr}_{E/F}$ and $N_{E/F}$ denote the trace and norm mappings, respectively, from E to F .

Let K be any finite field. We denote the multiplicative character group of K by \widehat{K} and the identity element of that group by χ_0 . If ψ is an additive character of K and $\chi \in \widehat{K}$, we denote the Gauss sum over K associated to these characters by $G_K(\chi, \psi)$. If e is the canonical additive character of K , we denote $G_K(\chi) = G_K(\chi, e)$. By notation e^a ($a \in K$) we mean the character defined by $e^a(x) = e(ax)$ for all $x \in K$.

We do not define $\chi(0)$, and consequently Gauss sums are calculated over K^* .

Let ψ be a non-trivial additive character of K . The orthogonality relations of characters, see [4, p. 195], imply

$$\psi(x) = \frac{1}{|K| - 1} \sum_{\chi \in \widehat{K}} G(\overline{\chi}, \psi) \chi(x) \quad \forall x \in K^*, \quad (2.1)$$

We shall also need the following two results:

Theorem 2.1. *Let $d \mid |K| - 1$, and let H denote the subgroup of order d of \widehat{K} . Then*

$$\sum_{x \in K^*} \psi(ax^d) = \sum_{\chi \in H} G(\overline{\chi}, \psi) \chi(a) \quad (= \sum_{\chi \in H} G(\chi, \psi) \overline{\chi}(a))$$

for all $a \in K^*$.

Proof. See [4, p. 217].

Lemma. Let γ be a primitive element of K , $a \in K$ and $d \mid |K| - 1$. Then

$$\sum_{x \in K^*} e(ax^d) = d \sum_{i=0}^{\frac{|K|-1}{d}-1} e(a\gamma^{di}) = d \sum_{x \in \langle \gamma^d \rangle} e(x).$$

Proof. Obvious.

Let $d \mid q - 1$ and H (resp. H') be the subgroup of order d of \widehat{F} (resp. \widehat{E}). The surjectivity of $N_{E/F}$ implies $H' = \{\chi \circ N_{E/F} \mid \chi \in H\}$.

Denote $N = N_{E/F}$. By Theorem 2.1 and the Davenport-Hasse theorem [4, p. 197-199], we now have

$$\sum_{x \in E^*} e_E(ax^d) = \sum_{\chi \in H} G_E(\bar{\chi} \circ N) \chi(N(a)) = (-1)^{m-1} \sum_{\chi \in H} G_F(\bar{\chi})^m \chi(N(a)). \quad (2.2)$$

Assume now that $d = q - 1$ and consequently $H = \widehat{F}$. Let $x_1, \dots, x_{m-1} \in F^*$ and denote $b = N(a)$. It follows from (2.1) that

$$e_F(bx_1^{-1} \dots x_{m-1}^{-1}) = \frac{1}{q-1} \sum_{\chi \in \widehat{F}} G_F(\bar{\chi}) \bar{\chi}(x_1) \dots \bar{\chi}(x_{m-1}) \chi(b).$$

By multiplying both sides of the preceding equation by $e_F(x_1 + \dots + x_{m-1})$ and by summing we obtain

$$\sum_{x_1, \dots, x_{m-1} \in F^*} e_F(x_1 + \dots + x_{m-1} + bx_1^{-1} \dots x_{m-1}^{-1}) = \frac{1}{q-1} \sum_{\chi \in \widehat{F}} G_F(\bar{\chi})^m \chi(b).$$

Thus we have proved

Theorem 2.2.

$$\sum_{x \in E^*} e(ax^{q-1}) = (-1)^{m-1} (q-1) K_{m-1}(N(a)) \quad \forall a \in E^*.$$

The surjectivity of N , the Weil bound and the Deligne bound, now imply

Corollary 2.3.

$$|K_m(a)| \leq \min\left\{q^{\frac{m+1}{2}} - \frac{q^{\frac{m+1}{2}} - 1}{q-1}, (m+1)q^{m/2}\right\} \quad \forall a \in F^*.$$

This result is, of course, valid for any non-trivial additive character ψ of F and also for sums

$$\sum_{x_1, \dots, x_{m-1} \in F^*} \psi(a_1 x_1 + \dots + a_m x_{m-1} + b x_1^{-1} \dots x_{m-1}^{-1}), \quad \forall a_i, b \in F^*.$$

Mordell [10] proved that $|K_m(a)| \leq q^{(m+1)/2}$, when q is prime. Thus our estimate generalizes and slightly improves this bound.

Corollary 2.4. *Let $a \in E^*$ and $d \mid q-1$. Then*

$$\left| \sum_{x \in E^*} e(ax^d) \right| \leq \min\{(d-1)q^{m/2} + 1, m(\sqrt{q} - 1/\sqrt{q})q^{m/2}\}.$$

Proof. Let γ be a primitive element of E . Denote $T = \langle \gamma^{q-1} \rangle$ and $t = (q-1)/d$. We now have a partition $\langle \gamma^d \rangle = \bigcup_{i=0}^{t-1} \gamma^{di} T$. By the Lemma and Theorem 2.2, we have

$$\sum_{x \in E^*} e(ax^d) = d \sum_{i=0}^{t-1} \sum_{x \in \gamma^{di} T} e(ax) = (-1)^{m-1} d \sum_{i=0}^{t-1} K_{m-1}(N_{E/F}(a\gamma^{di})).$$

The claim follows now from the Deligne bound and the Weil bound. \square

Next we shall consider certain exponential sums with binomial arguments. We need the following result which is a generalization of a result of C.J. Moreno and O. Moreno [11, Theorem 9].

We remark that the result can also be proved by using the results of R.J. McEliece in [8], where he used Gauss sums to determine the weight distributions of certain irreducible cyclic codes. We give, however, a direct proof for its simplicity and shortness. The proof rely on the 19th century theorem of Stickelberger, considering the values of certain Gauss sums [4, p. 202-203].

Assume $2 \mid m$. Then there exists an intermediate field M of E over F satisfying $[M : F] = 2$.

Theorem 2.5. *Let $a \in E^*$ and assume that m is even. If $d \mid q + 1$, then*

$$\sum_{x \in E} e(ax^d) = \begin{cases} (-1)^{m/2} q^{m/2} & \text{if } \text{ind } a \not\equiv k \pmod{d}, \\ (-1)^{m/2-1} (d-1) q^{m/2} & \text{if } \text{ind } a \equiv k \pmod{d}, \end{cases}$$

where $k = 0$ if

(1) $2 \mid q$; or $2 \nmid q$ and $m \equiv 0 \pmod{4}$; or $2 \nmid q$, $m \equiv 2 \pmod{4}$ and $2 \mid (q+1)/d$,

and $k = d/2$ if

(2) $2 \nmid q$, $m \equiv 2 \pmod{4}$ and $2 \nmid (q+1)/d$.

Proof. Let H be the subgroup of order d of \widehat{M} . By (2.2) we have

$$\sum_{x \in E} e(ax^d) = (-1)^{m/2-1} \sum_{\chi \in H^*} G_M(\overline{\chi})^{m/2} \chi(\mathbf{N}(a)),$$

where $H^* := H \setminus \{\chi_0\}$ and $\mathbf{N} := N_{E/M}$.

Let $\chi \in H^*$. Since $\text{ord}(\chi) \mid q + 1$, we observe that Stickelberg's theorem is applicable.

Now, if $2 \mid q$ or $2 \mid m/2$, then $G_M(\overline{\chi})^{m/2} = q^{m/2}$. To consider the remaining cases, we fix a generator of \widehat{M} , say λ , and denote $t = (q^2 - 1)/d$.

Now $\chi = \lambda^{tj}$ for some $j \in \{1, \dots, d-1\}$. Since $\text{ord}(\chi) = d/\text{gcd}(d, j)$, we see that $(q+1)/\text{ord}(\chi)$ is even, if $(q+1)/d$ is even. Consequently, $G_M(\overline{\chi})^{m/2} = q^{m/2}$, if $(q+1)/d$ is even.

Thus in the case (1) we have

$$\sum_{x \in E} e(ax^d) = (-1)^{m/2-1} q^{m/2} \sum_{j=1}^{d-1} \lambda^{tj}(\mathbf{N}(a)).$$

In the case (2) $(q+1)/\text{ord}(\chi)$ is even if and only if j is even. Thus

$$\sum_{x \in E} e(ax^d) = (-1)^{m/2-1} q^{m/2} \sum_{j=1}^{d-1} (-1)^j \lambda^{tj}(\mathbf{N}(a)).$$

By observing that, if γ is a primitive element of E then $\mathbf{N}(\gamma)$ is a primitive element of M , we easily obtain the result. \square

Proposition 2.6. *Assume that m is even. Then*

$$\sum_{x \in E^*} e(ax^{\frac{q^m-1}{q+1}}) = \begin{cases} q^m - 1 & \text{if } \text{Tr}_{E/M}(a) = 0, \\ -\frac{q^m - 1}{q + 1} K_1(\text{N}_{M/F}(\text{Tr}_{E/M}(a))) & \text{if } \text{Tr}_{E/M}(a) \neq 0. \end{cases}$$

Proof. Denote $\text{Tr} = \text{Tr}_{E/M}$, $\text{N} = \text{N}_{E/M}$ and $d = (q^m - 1)/(q + 1)$. As $e_E(ax^d) = e_M(\text{Tr}(a) \text{N}(x)^{q-1})$, we see that

$$\sum_{x \in E^*} e_E(ax^d) = \frac{q^m - 1}{q^2 - 1} \sum_{x \in M^*} e_M(\text{Tr}(a)x^{q-1}).$$

The claim follows now from Theorem 2.2. \square

Theorem 2.7. *Let $a, b \in E$, $b \neq 0$ and assume that m is even. Then*

$$\sum_{x \in E^*} e(ax^{\frac{q^m-1}{q+1}} + bx) = \begin{cases} -1 & \text{if } \text{Tr}_{E/M}(a) = 0, \\ (-1)^{\frac{m}{2}-1} e(\pm c) q^{\frac{m}{2}} + \frac{(-1)^{\frac{m}{2}-1} q^{\frac{m}{2}} + 1}{q + 1} K_1(h), & \text{if } \text{Tr}_{E/M}(a) \neq 0, \end{cases}$$

where $c = ab^{-(q^m-1)/(q+1)}$, $h = \text{N}_{M/F}(\text{Tr}_{E/M}(c))$ and the " $-$ " sign holds if and only if $2 \nmid q$ and $m \equiv 2 \pmod{4}$.

Proof. Denote $t = (q^m - 1)/(q + 1)$ and $\text{Tr} = \text{Tr}_{E/M}$. If $\text{Tr}(a) = 0$, then $e(ax^t) = e_M(\text{Tr}(a)x^t) = 1$ for all $x \in E$, and the claim follows. Assume that $\text{Tr}(a) \neq 0$.

Since the mapping $x \mapsto bx$ is a permutation of E^* , it is enough to consider sums

$$S := \sum_{x \in E^*} e(cx^t + x).$$

Let us fix a primitive element of E , say γ . Denote $T = \langle \gamma^{q+1} \rangle$. Now we have a partition $E^* = \bigcup_{j \in J} \gamma^j T$, where $J := \{0, \dots, q\}$. Denote $J^* = J \setminus \{k\}$, where $k = (q + 1)/2$ if $2 \nmid q$ and $m \equiv 2 \pmod{4}$, and otherwise $k = 0$. Now

$$S = \sum_{j \in J} e(c\gamma^{tj}) \sum_{x \in \gamma^j T} e(x) = e(\pm c) \sum_{x \in \gamma^k T} e(x) + \sum_{j \in J^*} e(c\gamma^{tj}) \sum_{x \in \gamma^j T} e(x),$$

where the " $-$ " sign holds if and only if $2 \nmid q$ and $m \equiv 2 \pmod{4}$. Since

$$\sum_{x \in \gamma^j T} e(x) = \frac{1}{q + 1} \sum_{x \in E^*} e(\gamma^j x^{q+1})$$

by the Lemma, it follows from Theorem 2.5 that

$$S = \frac{e(\pm c)((-1)^{m/2-1}q^{m/2+1} - 1)}{q+1} + \frac{(-1)^{m/2}q^{m/2} - 1}{q+1} \left(\sum_{j \in J} e(c\gamma^{tj}) - e(\pm c) \right).$$

The claim follows now easily from the Lemma and Proposition 2.6. \square

Consider next the sums

$$S(a, b) := \sum_{x \in E^*} e(ax^{\frac{q^m-1}{q-1}} + bx) \quad a, b \in E, \quad q > 1.$$

Assume $b \neq 0$. Again it is enough to consider sums $S(c, 1)$, where $c = ab^{-(q^m-1)/(q-1)}$. Denote $\text{Tr} = \text{Tr}_{E/F}$ and $N = N_{E/F}$. Assume that $\text{Tr}(a) \neq 0$. Let γ be a primitive element of E , and denote $T = \langle \gamma^{q-1} \rangle$ and $g = N(\gamma)$. Now

$$S(c, 1) = \sum_{i=0}^{q-2} e(cg^i) \sum_{x \in \gamma^i T} e(x).$$

It follows from the Lemma and Theorem 2.2 that

$$\sum_{x \in \gamma^i T} e(x) = (-1)^{m-1} K_{m-1}(g^i).$$

Thus

$$\begin{aligned} S(c, 1) &= (-1)^{m-1} \sum_{i=0}^{q-2} e_F(\text{Tr}(c)g^i) K_{m-1}(g^i) \\ &= (-1)^{m-1} \sum_{x_1, \dots, x_m \in F^*} e_F(x_1 + \dots + x_{m-1} + \text{Tr}(c)x_m + x_1^{-1} \dots x_{m-1}^{-1} x_m) \\ &= -1 + (-1)^{m-1} \sum_{x_1, \dots, x_{m-1} \in F^*} e_F(x_1 + \dots + x_{m-1}) \sum_{x_m \in F} e_F((\text{Tr}(c) + x_1^{-1} \dots x_{m-1}^{-1})x_m). \end{aligned}$$

The next two theorems follows now easily.

Theorem 2.8. *Let $a, b \in E$, $b \neq 0$. Then*

$$\sum_{x \in E^*} e(ax^{q+1} + bx) = \begin{cases} -1 & \text{if } a + a^q = 0, \\ -qe_F(-b^{q+1}(a + a^q)^{-1}) - 1 & \text{if } a + a^q \neq 0. \end{cases}$$

Theorem 2.9. *Let $a, b \in E$, $b \neq 0$. Assume that $m > 2$. Then*

$$\sum_{x \in E^*} e(ax \frac{q^m - 1}{q - 1} + bx) = \begin{cases} -1 & \text{if } \text{Tr}_{E/F}(a) = 0, \\ (-1)^{m-1} q K_{m-2}(-N_{E/F}(b) \text{Tr}_{E/F}(a)^{-1}) - 1 & \text{if } \text{Tr}_{E/F}(a) \neq 0. \end{cases}$$

The discussion concerning sums $S(a, b)$ is completed by a (trivial)

Proposition 2.10. *If $q > 2$ then*

$$\sum_{x \in E^*} e(ax \frac{q^m - 1}{q - 1}) = \begin{cases} q^m - 1 & \text{if } \text{Tr}_{E/F}(a) = 0, \\ -\frac{q^m - 1}{q - 1} & \text{if } \text{Tr}_{E/F}(a) \neq 0. \end{cases}$$

Remark. From the result of Theorem 2.8 it is easy to determine the distribution of the even correlations of a set of PN-sequences, so called small Kasami set, both in binary and non-binary cases. (c.f. [2], [6]).

3. Three examples

Let us first consider some basic facts about the *trace codes*. For a more complete description see [2].

We restrict our considerations to the binary trace codes. Let K be the finite field with 2^k elements and fix a primitive element of K , say γ . Let Tr denote the trace mapping from K to the prime field \mathbb{F}_2 . Let P be an additive subgroup of $K[X]$ and $n \in \mathbb{Z}_+$. Define a trace code $C(P) := \{c(f) \mid f \in P\}$, where $c(f) = (\text{Tr}(f(1)), \text{Tr}(f(\gamma)), \dots, \text{Tr}(f(\gamma^{n-1})))$ and $n \in \mathbb{Z}_+$. It is easy to see that $wt(c)$, the (Hamming) weight of a codeword $c \in C(P)$, is equal to $\frac{1}{2}(n - \sum_{i=0}^{n-1} e_K(f(\gamma^i)))$ [2].

The next theorem is also from [2].

Theorem 3.1. *Set $2^k - 1 = nN$. The dual of the binary cyclic code B of length n with zeros $\gamma^{Ns_1}, \dots, \gamma^{Ns_u}$ is the code $C(P)$, where $P = \{\sum_{i=1}^u a_i x^{Ns_i} \mid a_i \in K\}$.*

Let $q = 2^r$. Choose $K = \mathbb{F}_{q^m}$ and $P = \{ax^{q-1} \mid a \in K\}$. It follows from Theorem 3.1 that the dual of the binary cyclic code of length $n = (q^m - 1)/(q - 1)$ with zeroes

$\gamma^{(q-1)2^i}$, $i = 1, 2, \dots$ is the code $C(P)$. It is easy to see that $\text{ord}_n(2) = rm$. Thus $C(P)$ is an irreducible cyclic code of dimension rm [5, p. 77-78]. Since

$$\sum_{i=0}^{n-1} e(a\gamma^{(q-1)^i}) = \frac{1}{q-1} \sum_{x \in K^*} e(ax^{q-1})$$

by the Lemma, it follows from Theorem 2.2 and Corollary 2.4, that

$$|2wt(c) - \frac{q^m - 1}{q - 1}| \leq \min\{mq^{(m-1)/2}, \sqrt{q}q^{(m-1)/2} - \frac{q^{m/2} - 1}{q - 1}\}$$

for all $c \in C(P) \setminus \{(0, \dots, 0)\}$.

In the case $m = 2$, $C(P)$ is the dual of the Zetterberg code [7, p. 206]. This dual has been studied at least in [9] and [3].

Let us assume that m is even. Denote $d = (q^m - 1)/(q + 1)$, and choose $K = \mathbb{F}_{q^m}$ and $P = \{ax^d + bx \mid a, b \in K\}$. The dual of the binary cyclic code of length $q^m - 1$ with zeroes $\gamma^{d2^i}, \gamma^{2^i}$, $i = 1, 2, \dots$ is the code $C(P)$.

Denote $P_1 = \{bx \mid b \in K\}$ and $P_2 = \{ax^d \mid a \in K\}$. The weight of any non-zero codeword of the code $C(P_1)$ is equal to q^{m-1} . By Proposition 2.6 and the Deligne bound there is no codeword of that weight in the code $C(P_2)$. Since $C(P_1)$ and $C(P_2)$ are subgroups of $C(P)$ we have $C(P) = C(P_1) \oplus C(P_2)$. Obviously $|C(P_1)| = q^m$, and by Proposition 2.6 $|C(P_2)| = q^2$. Thus $|C(P)| = q^{m+2}$. By Proposition 2.6, Theorem 2.7 and the Deligne bound, we know now that there are

- (1) $q^m - 1$ codewords of weight $q^m/2$ in the code $C(P)$,
- (2) $q^2 - 1$ codewords c whose weights satisfy

$$\frac{q^m - 1}{q + 1} \leq |2wt(c) - q^m + 1| \leq 2\sqrt{q}\frac{q^m - 1}{q + 1},$$

- (3) $(q^2 - 1)q^m - q^2 + 1$ codewords c whose weights satisfy

$$|2wt(c) - q^m + 1| \leq q^{m/2} + 2\sqrt{q}\frac{q^{m/2} + 1}{q + 1}.$$

We remark that $C(P_1)$ is the simplex code of length $q^m - 1$, and $C(P_2)$ is the code constructed by pasting together d copies of each codewords of the dual of the Zetterberg code of length $q + 1$.

Let us assume that $q > 2$ and $m > 2$. Denote $d = (q^m - 1)/(q - 1)$, and choose $K = \mathbb{F}_{q^m}$ and $P = \{ax^d + bx \mid a, b \in K\}$. Now $C(P)$ is the dual of the binary cyclic code of length $q^m - 1$ with zeroes $\gamma^{d2^i}, \gamma^{2^i}, i = 1, 2, \dots$

Denote $P_1 = \{bx \mid b \in K\}$ and $P_2 = \{ax^d \mid a, b \in K\}$. Again $C(P) = C(P_1) \oplus C(P_2)$, and $|C(P_1)| = q^m$. By Proposition 2.10 $|C(P_2)| = q$. Thus $|C(P)| = q^{m+1}$. By Theorem 2.9, Proposition 2.10 and Corollary 2.3, we now know that there are

- (1) $q^m - 1$ codewords of weight $q^m/2$,
- (2) $q - 1$ codewords of weight $(q^m - 1 + (q^m - 1)/(q - 1))/2$.

in the code $C(P)$.

For the remaining $(q - 1)q^m - q + 1$ non-zero codewords $c \in C(P)$ it holds that

- (3) $q - 1 \leq |2wt(c) - q^m + 1| \leq \min\{q^{\frac{m+1}{2}} - \frac{q^{\frac{m+1}{2}} - q}{q-1} + 1, (m + 1)q^{m/2}\}$.

We remark that $C(P_1)$ is again the binary simplex code of length $q^m - 1$, and $C(P_2)$ is the code constructed by pasting together d copies of each codewords of the binary simplex code of length $q - 1$.

REFERENCES

1. Deligne P. (1977) Applications de la formule des traces aux sommes trigonometriques. SGA 4 1/2 Springer Lecture Notes in Math 569: 168-232. Springer, New York.
2. Honkala I. & Tietäväinen A. Codes and Number Theory. In Brualdi R. A., Huffman W. C. & Pless V. (ed) Handbook of Coding Theory. Elsevier Science Publisher, Amsterdam. In Preparation.
3. Lachaud G. & Wolfman J. (1990) The weights of the orthogonals of the extended quadratic binary Goppa codes. IEEE Trans. Inform. Theory 36: 686-692.
4. Lidl R. & Niederreiter H. (1984) Finite Fields. Cambridge Univ. Press, Cambridge.

5. van Lint J. H. (1982) Introduction to Coding Theory. Springer-Verlag, New York.
6. Liu S. C. and Komo J. J. (1992) Nonbinary Kasami sequences over $GF(p)$. IEEE Trans. Inform. Theory 38: 1409-1412.
7. MacWilliams F. J. & Sloane N. J. A (1978) The Theory of Error-Correcting Codes. North-Holland, Amsterdam.
8. McEliece R.J. (1974) Irreducible cyclic codes and Gauss sums. In: Hall M. Jr. & van Lint J.H. (ed) Combinatorics (Part 1): 179-196. Mathematical Centre Tracts 55, Mathematical Centre, Amsterdam.
9. McEliece R. J. (1980) Correlation properties of sets of sequences derived from irreducible cyclic codes. Inform. and Control 45: 18-25.
10. Mordell L. J. (1963) On a special polynomial congruence and exponential sums. In: Calcutta Math. Soc. Golden Jubilee Commemoration Volume, Part 1: 29-32. Calcutta Math. Soc., Calcutta.
11. Moreno C. J. & Moreno O. (1994) The MacWilliams-Sloane conjecture on the tightness of the Carlitz-Uchiyama bound and the weights of duals of BCH codes. IEEE Trans. Inform. Theory 40: 1894-1907.
12. Weil A. (1948) On some exponential sums. Proc. Nat. Ac. Sc. 34: 204-207.