Kloosterman sum identities and low-weight codewords in a cyclic code with two zeros

Marko Moisio\textsuperscript{a}, Kalle Ranto\textsuperscript{b,*}\textsuperscript{,1}

\textsuperscript{a} Department of Mathematics and Statistics, University of Vaasa, PO Box 700, FIN-65101 Vaasa, Finland
\textsuperscript{b} Department of Mathematics, University of Turku, FIN-20014 Turku, Finland

Received 15 November 2005; revised 12 April 2006
Available online 21 June 2006
Communicated by Gary L. Mullen

Abstract

We apply relations of \(n\)-dimensional Kloosterman sums to exponential sums over finite fields to count the number of low-weight codewords in a cyclic code with two zeros. As a corollary we obtain a new proof for a result of Carlitz which relates one- and two-dimensional Kloosterman sums. In addition, we count some power sums of Kloosterman sums over certain subfields.

© 2006 Elsevier Inc. All rights reserved.

Keywords: \(n\)-Dimensional Kloosterman sum; Kloosterman sum; Exponential sum; Cyclic code

1. Introduction

Let \(\mathbb{F}_{p^n}\) be the finite field with \(p^n\) elements with a primitive element \(\gamma\). We consider \(p\)-ary cyclic codes \(C_{1,t}\) of length \(p^n - 1\) with two zeros \(\gamma\) and \(\gamma^t\), that is, codes defined by a parity-check matrix

\[
\begin{pmatrix}
1 & \gamma & \gamma^2 & \ldots & \gamma^{p^n - 2} \\
1 & \gamma^t & \gamma^{2t} & \ldots & \gamma^{(p^n - 2)t}
\end{pmatrix}
\]

* Corresponding author.

E-mail addresses: mamo@uwasa.fi (M. Moisio), kara@utu.fi (K. Ranto).

\textsuperscript{1} Research supported by the Academy of Finland (Grant 108238).
These codes have been studied extensively but still several open problems remain [3, Section 3.4.2]. The minimum distance of these codes is known to be in the range 3–5 but the exact value is known only for some special cases, see e.g. [5]. The number of low-weight codewords is known for even fewer codes.

In this paper we count the number of codewords of weight 3 and 4 in $C_{1,t}$ with specific choices $p = 2$, $n = 3r$ and $t = (2^{3r} - 1)/(2^r - 1) = 2^{2r} + 2^r + 1$. These codes have parameters $[2^n - 1, 2^n - 1 - 4r, 3]$ (see Section 7) and for the length 511 the weight distribution of the dual code can be found from [3, p15 in Table 8].

When $\gcd(t, p^n - 1) = 1$ counting the number of codewords of weight 3 in $C_{1,t}$ is the same problem as counting the third power sum for cross-correlation function of $m$-sequences with decimation $t$. In both problems one wishes to count the number of solutions $x \in F_{p^n}$ to the equation

$$(x + 1)^t = x^t + 1.$$ 

Actually, we are able to count the number of solutions $x \in F_{p^n}$ to the equation

$$(x - \beta)^t = x^t - \alpha \quad \forall \alpha, \beta \in F_{p^n}, \quad (1)$$

for every $p$ with $n = 3r$ and $t = (p^{3r} - 1)/(p^r - 1) = p^{2r} + p^r + 1$. When $p = 2$, we obtain as a corollary results on certain power sums of Kloosterman sums which opens up a possibility to calculate the number of low-weight codewords.

Quite recently, a sum of squares of Kloosterman sums, where the outer sum is calculated over the quadratic subfield of the field in which the Kloosterman sum is defined, has been calculated by Charpin, Helleseth, and Zinoviev in [4]. We give another proof for this result with our method and generalize it in two ways.

The paper is structured as follows. In Section 2 we recall two results by the first author relating $n$-dimensional Kloosterman sums to exponential sums. These are needed in Section 3 to count the solutions of (1). In Section 4 we derive some straightforward corollaries to the main result of Section 3 and use them in Sections 5 and 6 to count some power sums of Kloosterman sums over subfields. Finally, in Section 7, we calculate the number of codewords of weight 3 and 4 in $C_{1,t}$.

### 2. Identities of $n$-dimensional Kloosterman sums

For the rest of this paper we let $q = p^r$ and $t = (q^m - 1)/(q - 1) = q^{m-1} + \cdots + q + 1$ for some integer $m \geq 2$. We consider the finite fields $F_q$ and $F_{q^m}$ and the following basic functions on them.

**Definition 1.** We use the following notation:

\[
\begin{align*}
\text{tr}(x) &= x + x^p + \cdots + x^{p^{r-1}} & \text{the absolute trace function } F_q \to F_p, \\
\text{Tr}(x) &= x + x^q + \cdots + x^{q^{m-1}} & \text{the relative trace function } F_{q^m} \to F_q, \\
N(x) &= x^{1+q+\cdots+q^{m-1}} = x^t & \text{the relative norm function } F_{q^m} \to F_q, \\
\chi(x) &= e^{2\pi i / p} \text{tr}(x) & \text{the canonical additive character of } F_q,
\end{align*}
\]


where \( e(x) = e^{\frac{2\pi i}{p} \text{tr}(x)} \) is the canonical additive character of \( \mathbb{F}_{q^m} \),

\[ \eta(x), \quad \text{with } \eta(0) = 0, \quad \text{the quadratic character of } \mathbb{F}^*_q, \quad q \text{ odd.} \]

We present a well-known result, sometimes called the orthogonality of characters, as a lemma for later reference.

**Lemma 2.** For any \( a \in \mathbb{F}_q \)

\[
\sum_{x \in \mathbb{F}_q} \chi(ax) = \begin{cases} q, & \text{if } a = 0; \\ 0, & \text{if } a \neq 0. \end{cases}
\]

Of course, similar results hold for all characters, e.g. for \( e(x) \) of \( \mathbb{F}_{q^m} \). In addition, this lemma implies immediately

\[
\sum_{x_1, \ldots, x_s \in \mathbb{F}^*_q} \chi(x_1 + \cdots + x_s) = \left( \sum_{x \in \mathbb{F}^*_q} \chi(x) \right)^s = (-1)^s. \tag{2}
\]

The next two propositions from [10] are in a central role in our study of Eq. (1). Let

\[ k_n(a) = \sum_{x_1, \ldots, x_n \in \mathbb{F}^*_q} \chi(x_1 + \cdots + x_n + ax_1^{-1} \cdots x_n^{-1}) \]

be the \( n \)-dimensional Kloosterman sum over \( \mathbb{F}^*_q \) with \( a \in \mathbb{F}^*_q \).

**Proposition 3.**

\[
\sum_{x \in \mathbb{F}^*_q} e(\alpha x^{q+1}) = (-1)^{m-1}(q - 1)k_{m-1}(N(\alpha)) \quad \forall \alpha \in \mathbb{F}^*_q.
\]

An interested reader can find the proof also from [11, Theorem 3], where it is proved by using Gauss sums, Davenport–Hasse identity, and a discrete (inverse) Fourier transform.

For the convenience of the reader we prove the following proposition also here.

**Proposition 4.** Let \( \alpha, \beta \in \mathbb{F}_{q^m}, \beta \neq 0, \) and \( m > 2 \). Then

\[
\sum_{x \in \mathbb{F}^*_q} e(\alpha x^t + \beta x) = \begin{cases} 0, & \text{if } \text{Tr}(\alpha) = 0; \\ (-1)^{m-1}qk_{m-2}(-N(\beta)/\text{Tr}(\alpha)), & \text{if } \text{Tr}(\alpha) \neq 0. \end{cases}
\]

**Proof.** If \( \text{Tr}(\alpha) = 0, e(\alpha x^t) = \chi(\text{Tr}(\alpha)x^t) = 1 \) and the claim follows. Assume \( \text{Tr}(\alpha) \neq 0. \) Let \( \gamma \) be a generator of \( \mathbb{F}^*_{q^m} \) and consider the partition

\[
\mathbb{F}^*_{q^m} = \bigcup_{i=0}^{q-2} \gamma^{q^{-1}} \gamma^i.
\]
Since $t = (q^m - 1)/(q - 1)$ we obviously have

$$S := \sum_{x \in \mathbb{F}_q^m} e(\alpha x^t + \beta x) = \sum_{i=0}^{q-2} e(\alpha \gamma^i) \sum_{j=0}^{t-1} e(\beta \gamma^i \gamma(q-1)j).$$

By Proposition 3 the inner sum equals

$$\sum_{j=0}^{t-1} e(\beta \gamma^i \gamma(q-1)j) = \frac{1}{q-1} \sum_{x \in \mathbb{F}_q^m} e(\beta \gamma^i x^{q-1}) = (-1)^{m-1} k_{m-1}(N(\beta) N(\gamma)^i).$$

Let $g := N(\gamma) = \gamma^t$ which is a primitive element of $\mathbb{F}_q$. Now

$$S = (-1)^{m-1} \sum_{i=0}^{q-2} \chi(\text{Tr}(\alpha) g^i) k_{m-1}(\beta^i g^i)$$

$$= (-1)^{m-1} \sum_{x_1, \ldots, x_m \in \mathbb{F}_q^*} \chi(\text{Tr}(\alpha) x_m + x_1 + \cdots + x_{m-1} + \beta^i x_m x_1^{-1} \cdots x_{m-1}^{-1})$$

$$= -1 + (-1)^{m-1} \sum_{x_1, \ldots, x_{m-1} \in \mathbb{F}_q^*} \chi(x_1 + \cdots + x_{m-1})$$

$$\times \sum_{x_m \in \mathbb{F}_q} \chi(x_m (\text{Tr}(\alpha) + \beta^i x_1^{-1} \cdots x_{m-1}^{-1})).$$

By Lemma 2 the inner sum above equals $q$ if $x_{m-1} = -\beta^i \text{Tr}(\alpha)^{-1} x_1^{-1} \cdots x_{m-2}^{-1}$, and otherwise it equals 0. Hence,

$$S = (-1)^{m-1} q \sum_{x_1, \ldots, x_{m-2} \in \mathbb{F}_q^*} \chi(x_1 + \cdots + x_{m-2} - \beta^i \text{Tr}(\alpha)^{-1} x_1^{-1} \cdots x_{m-2}^{-1}) - 1. \quad \Box$$

3. The number of solutions of $x^t + (\beta - x)^t = \alpha$

As before, let $q = p^r$ for any prime $p$. From now on we assume that $m = 3$ which gives $t = q^2 + q + 1$. Recall that $\eta(x)$ is the quadratic character of $\mathbb{F}_q^*$ when $q$ is odd. We are now able to prove our key result:

**Theorem 5.** Let $a \in \mathbb{F}_q$ and $\beta \in \mathbb{F}_q^*$. The number of solutions $x \in \mathbb{F}_q^3$ of the equation

$$x^t + (\beta - x)^t = a$$

is equal to

$$N = \begin{cases} 
q^2 + \chi(a) q, & \text{if } q \text{ is even;} \\
q^2 + \eta(1 - 4 a/p) q, & \text{if } q \text{ is odd.}
\end{cases}$$
Proof. Let \( a \in F_q^* \) and choose \( \alpha \in F_q^* \) such that \( \text{Tr}(\alpha) = -a \). Let \( \beta \in F_q^* \) and let \( \delta \) be an element of \( F_q^* \) satisfying \( \text{Tr}(\delta) = 1 \). Now, by Proposition 4, we have

\[
\sum_{u \in F_q^*} \left( \sum_{x \in F_q^*} e(\alpha x^t + u\beta x) \right) \left( \sum_{y \in F_q^*} e(\delta y^t - uy) \right) \left( \sum_{z \in F_q^*} e(\delta z^t - uz) \right) = q^3 \sum_{u \in F_q^*} \left( \sum_{b \in F_q^*} \chi(b^{-1} + a^{-1}u^t\beta^t b) \right) \left( \sum_{c \in F_q^*} \chi(c^{-1} + u^t c) \right) \left( \sum_{d \in F_q^*} \chi(d^{-1} + u^t d) \right).
\]

For example, the sum \( \sum_{x \in F_q^3} e(\alpha x^t + u\beta x) \) is equal to \( qk_1(-u\beta)^t/(-a) \) by Proposition 4 as \( a \neq 0 \). This Kloosterman sum is defined to be \( q \sum_{b \in F_q^*} \chi(b + a^{-1}u^t\beta^t b^{-1}) \) and here we can change the roles of \( b \) and \( b^{-1} \).

Let \( S_1 \) and \( S_2 \) denote the lhs and rhs of the preceding equation. Now

\[
S_1 = \sum_{u \in F_q^*} \sum_{x,y,z \in F_q^3} e(\alpha x^t + \delta y^t + \delta z^t + u(\beta x - y - z)) - \sum_{x,y,z \in F_q^3} e(\alpha x^t + \delta y^t + \delta z^t)
\]

where the last sum equals \( (1 - t)^3 \) as \( x \mapsto x^t = N(x) \) is \( t \)-to-1 function from \( F_q^* \) onto \( F_q^* \), and by Lemma 2

\[
\sum_{x \in F_q^3} e(\alpha N(x)) = t \sum_{u \in F_q^*} \chi(\text{Tr}(\alpha)u) + 1 = -t + 1. \tag{3}
\]

Hence,

\[
S_1 = \sum_{x,y,z \in F_q^3} e(\alpha x^t + \delta y^t + \delta z^t) \sum_{u \in F_q^*} e(u(\beta x - y - z)) + (t - 1)^3.
\]

By Lemma 2 the inner sum equals \( q^3 \) if \( z = \beta x - y \), and otherwise it equals 0. Thus, by the substitution \( y = vx \)

\[
S_1 = q^3 \sum_{x,y \in F_q^3} e(\alpha x^t + \delta y^t + \delta(\beta x - y)^t) + (t - 1)^3
\]

\[
= q^3 \sum_{v \in F_q^3} \sum_{x \in F_q^3} e(x^t(\alpha + \delta(v^t + (\beta - v)^t))) + (t - 1)^3.
\]

Again, by Lemma 2 the inner sum equals \( q^3 \) if \( \text{Tr}(\alpha + \delta(v^t + (\beta - v)^t)) = 0 \) and otherwise it equals \( 1 - t \). But \( v^t + (\beta - v)^t \) belongs to \( F_q^* \) for all \( v \in F_q^3 \), and therefore we have \( \text{Tr}(\alpha + \delta(v^t + (\beta - v)^t)) = 0 \) iff \( \text{Tr}(\delta)(v^t + (\beta - v)^t) = -\text{Tr}(\alpha) \) iff \( v^t + (\beta - v)^t = a \). Now, since \( t - 1 = q(q + 1) \) we obtain
\[ S_1 = q^6 N + q^3 (q^3 - N)(1 - t) + (t - 1)^3 \]
\[ = q^3 (q^3 N + (N - q^3)q(q + 1) + (q + 1)^3) = q^3 t(qN - q^3 + 2q + 1) \]

where \( N \) is the number of solutions in the claim.

Next we calculate \( S_2 \) and remember that \( u \mapsto u' \) is \( t \)-to-1 mapping

\[ S_2 = q^3 \sum_{u \in \mathbb{F}_q^*} \sum_{b,c,d \in \mathbb{F}_q^*} \chi(b^{-1} + c^{-1} + d^{-1} + u'((a^{-1} \beta' b + c + d))) \]
\[ = q^3 \sum_{b,c,d \in \mathbb{F}_q^*} \chi(b^{-1} + c^{-1} + d^{-1}) \sum_{u \in \mathbb{F}_q^*} \chi(u'((a^{-1} \beta' b + c + d))) \]
\[ = q^3 t \sum_{b,c,d \in \mathbb{F}_q^*} \chi(b^{-1} + c^{-1} + d^{-1}) \sum_{g \in \mathbb{F}_q^*} \chi(g(a^{-1} \beta' b + c + d)) \]
\[ - q^3 t \sum_{b,c,d \in \mathbb{F}_q^*} \chi(b^{-1} + c^{-1} + d^{-1}). \]

By (2), Lemma 2, and the substitution \( c = bf \) we have

\[ S_2 = q^4 t \sum_{b,c \in \mathbb{F}_q^*} \sum_{a^{-1} \beta' b + c \neq 0} \chi(b^{-1} + c^{-1} - (a^{-1} \beta' b + c)^{-1}) + q^3 t \]
\[ = q^4 t \sum_{f \in \mathbb{F}_q^*} \sum_{b \in \mathbb{F}_q^*} \chi(b^{-1}(1 + f^{-1} - (a^{-1} \beta' + f)^{-1})) + q^3 t. \]

Finally, by Lemma 2 the inner sum equals \( q - 1 \) if \( 1 + f^{-1} - (a^{-1} \beta' + f)^{-1} = 0 \) and otherwise it equals \(-1\). As \( f \neq 0 \) and \( f \neq -a^{-1} \beta' \neq 0 \) we get

\[ S_2 = q^4 t (q - 1)N' - q^4 t(q - 2 - N') + q^3 t = q^3 t((N' - 1)q^2 + 2q + 1), \]

where

\[ N' = |\{ f \in \mathbb{F}_q^* | 1 + f^{-1} - (a^{-1} \beta' + f)^{-1} = 0 \}|. \]

As we have \( S_1 = S_2 \), we get

\[ N = q^2 + (N' - 1)q. \]

Since \( 1 + f^{-1} - (a^{-1} \beta' + f)^{-1} = 0 \) iff \( (f + 1)/f = 1/(a^{-1} \beta' + f) \) iff \( f^2 + a^{-1} \beta' f + a^{-1} \beta' = 0 \)
iff \( g^2 + g + a \beta^{-t} = 0 \) where \( g = a \beta^{-t} f \), we obtain

\[ N' = \begin{cases} 
1 + \chi(\frac{g}{\beta'}), & \text{if } q \text{ is even}; \\
1 + \eta(1 - 4 \frac{g}{\beta'}), & \text{if } q \text{ is odd}; 
\end{cases} \]
see e.g. [9, Exercise 5.24], and the claim follows in the case \(a \neq 0\). Moreover, \(x^t + (\beta - x)^t = 0\) iff \((1 - \beta/x)^t = 1\). Since \(\text{Im}(1 - \beta/x) = F_{qm} \setminus \{1\}\) it follows that \(N = t - 1\) and the claim holds also when \(a = 0\). □

4. A result of Carlitz

From now on we assume that \(p = 2\), i.e., \(q = 2^r\) for some \(r\) and \(t = q^2 + q + 1\). We could formulate the following theorem also in the case \(p > 2\) but it becomes somewhat more complicated and in the next three sections we need only the binary case.

**Theorem 6.** Let \(q\) be even and \(\beta, \delta \in F_{q^3}\). Then

\[
\sum_{x \in F_{q^3}^*} e\left(\delta (x^t + (\beta + x)^t)\right) = \begin{cases} 
q^3, & \text{if } \text{Tr}(\delta)\beta = 0; \\
q^2, & \text{if } \beta^{-t} = \text{Tr}(\delta); \\
0, & \text{if } \beta^{-t} \neq \text{Tr}(\delta).
\end{cases}
\]

**Proof.** If \(\text{Tr}(\delta)\beta = 0\), the claim is clear. Let \(S\) denote the above sum and let \(N_a\) be the number of solutions of \(x^t + (\beta + x)^t = a\) in \(F_{q^3}^*\). By Theorem 5, we have

\[
S = \sum_{x \in F_{q^3}^*} \chi(\text{Tr}(\delta)(x^t + (\beta + x)^t)) = \sum_{a \in F_q} N_a \chi(\text{Tr}(\delta)a)
\]

\[
= \sum_{a \in F_q} (q^2 + \chi(a\beta^{-t})) \chi(\text{Tr}(\delta)a) = q^2 \sum_{a \in F_q} \chi(a) + q \sum_{a \in F_q} \chi(a(\beta^{-t} + \text{Tr}(\delta))
\]

and now the claim follows from Lemma 2. □

We can now prove a result of Carlitz [1] as a corollary.

**Corollary 7.** If \(q\) is even, then

\[
k_2(a) = k_1(a)^2 - q \quad \forall a \in F_q^*.
\]

**Proof.** We calculate the square \(S = (\sum_{x \in F_{q^3}^*} e(x^t + \alpha x))^2\) with \(\alpha \in F_{q^3}^*\) in two ways. On one hand, by Theorem 6 and Proposition 3

\[
S = \sum_{x, y \in F_{q^3}^*} e(x^t + y^t + \alpha(x + y)) = \sum_{z \in F_{q^3}^*} e(\alpha z) \sum_{x \in F_{q^3}^*} e(x^t + (x + z)^t)
\]

\[
= q^3 + \sum_{z \in F_{q^3}^*} e(\alpha z) \sum_{x \in F_{q^3}^*} e(x^t + (x + z)^t) = q^3 + q^2 \sum_{z \in (F_{q^3}^*)^{q-1}} e(\alpha z)
\]

\[
= q^3 + q^2 \frac{1}{q-1} \sum_{z \in F_{q^3}^*} e(\alpha z^{q-1}) = q^3 + q^2 (-1)^2 k_2(a')
\]

where \((F_{q^3}^*)^{q-1}\) is the subgroup of \(F_{q^3}^*\) consisting of \((q - 1)\)th powers.
On the other hand, by Proposition 4, we have $S = q^2 k_1(\alpha^i)^2$. □

**Remark 8.** Let $q$ be even. Lachaud and Wolfmann [7] have proved that

$$\{k_1(a) \mid a \in \mathbb{F}_q^* \} = \{i \mid i \in [-2\sqrt{q}, 2\sqrt{q}], \ i \equiv -1 \ (\text{mod} \ 4) \}.$$  

By Corollary 7 we get immediately

$$\{k_2(a) \mid a \in \mathbb{F}_q^* \} = \{i^2 - q \mid i \in [-2\sqrt{q}, 2\sqrt{q}], \ i \equiv -1 \ (\text{mod} \ 4) \}$$

and hence $1 - q \leq k_2(a) \leq 3q$.

5. **Power sums of Kloosterman sums**

The (one-dimensional) Kloosterman sum can be seen as a cross-correlation function of two $m$-sequences that differ by a decimation $-1$. By, e.g., [6, Theorem 3.2] we have the following result.

**Proposition 9.** If $q = 2^r$, then

$$\sum_{a \in \mathbb{F}_q^*} k_1(a) = 1, \quad \sum_{a \in \mathbb{F}_q^*} k_1(a)^2 = q^2 - q - 1, \quad \text{and} \quad \sum_{a \in \mathbb{F}_q^*} k_1(a)^3 = (-1)^r q^2 + 2q + 1.$$  

Next we calculate the fourth power sum of Kloosterman sums which is needed to count the codewords of weight 4 in the cyclic codes $C_{1,t}$.

**Corollary 10.** If $q$ is even, then

$$\sum_{a \in \mathbb{F}_q^*} k_1(a)^4 = 2q^3 - 2q^2 - 3q - 1.$$  

**Proof.** By Corollary 7 we have

$$\sum_{a \in \mathbb{F}_q^*} k_1(a)^4 = \sum_{a \in \mathbb{F}_q^*} (k_2(a) + q)^2 = \sum_{a \in \mathbb{F}_q^*} k_2(a)^2 + 2\sum_{a \in \mathbb{F}_q^*} k_2(a) + \sum_{a \in \mathbb{F}_q^*} q^2.$$  

Firstly, we calculate the easier sum using Lemma 2

$$\sum_{a \in \mathbb{F}_q^*} k_2(a) = \sum_{a,x,y \in \mathbb{F}_q^*} \chi(x + y + ax^{-1}y^{-1})$$

$$= \sum_{x,y \in \mathbb{F}_q^*} \chi(x + y) \sum_{a \in \mathbb{F}_q} \chi(ax^{-1}y^{-1}) - \sum_{x,y \in \mathbb{F}_q^*} \chi(x + y)$$

$$= -\sum_{x \in \mathbb{F}_q^*} \chi(x) \sum_{y \in \mathbb{F}_q} \chi(y) = (-1)^3 = -1.$$
Secondly, we calculate the other sum using Lemma 2 and (2)

\[ \sum_{a \in \mathbb{F}_q^*} k_2(a)^2 = \sum_{a, x, y, z, w \in \mathbb{F}_q^*} \chi(x + y + z + w + ax^{-1}y^{-1} + az^{-1}w^{-1}) \]

\[ = \sum_{x, y, z, w \in \mathbb{F}_q^*} \chi(x + y + z + w) \sum_{a \in \mathbb{F}_q^*} \chi(a(x^{-1}y^{-1} + z^{-1}w^{-1})) \]

\[ - \sum_{x, y, z, w \in \mathbb{F}_q^*} \chi(x + y + z + w) \]

\[ = q \sum_{x, y, z, w \in \mathbb{F}_q^*} \chi(x + y + z + w) - 1 \]

\[ = q \sum_{y, z \in \mathbb{F}_q^*} \chi(y + z) \sum_{x \in \mathbb{F}_q^*} \chi(x(1 + yz^{-1})) - q(-1)^2 - 1 \]

\[ = q^2 \sum_{y = z \in \mathbb{F}_q^*} \chi(y + z) - q - 1 = q^2(q - 1) - q - 1. \]

The sum in the claim is then equal to \( (q^3 - q^2 - q - 1) - 2q + q^2(q - 1). \)

\[ \square \]

**Remark 11.** This corollary is equivalent to [4, Proposition 1] recently proved by Charpin, Helle-seth, and Zinoviev in a different way. Actually, they have also proved the above result of Carlitz in [4, Proposition 2] (without noticing this connection) but they do not use it to prove the previous corollary.

We can count also the sixth power sum of Kloosterman sums but before that we need a lemma. This result follows easily from Propositions 1 and 2 in [11].

**Lemma 12.** If \( q = 2^r \), then

\[ \sum_{a \in \mathbb{F}_q^*} k_2(a)^3 = q^4 - q^3 - (-1)^r q^3 - 3q^2 - 2q - 1. \]

**Theorem 13.** If \( q = 2^r \), then

\[ \sum_{a \in \mathbb{F}_q^*} k_1(a)^6 = 5q^4 - 5q^3 - (-1)^r q^3 - 9q^2 - 5q - 1. \]

**Proof.** By Corollary 7, the proof of Corollary 10, and Lemma 12 we have

\[ \sum_{a \in \mathbb{F}_q^*} k_1(a)^6 = \sum_{a \in \mathbb{F}_q^*} (q + k_2(a))^3 = \sum_{a \in \mathbb{F}_q^*} (q^3 + 3q^2k_2(a) + 3qk_2(a)^2 + k_2(a)^3) \]

\[ = q^3(q - 1) - 3q^2 + 3q(q^3 - q^2 - q - 1) \]

\[ + q^4 - q^3 - (-1)^r q^3 - 3q^2 - 2q - 1. \]

\[ \square \]
Remark 14. From Theorem 13 we derive immediately an elementary non-trivial bound for Kloosterman sums over any finite field $F_q$ with $q$ even:

$$\left| k_1(a) \right| \leq 5^{1/6} q^{-2/3} < 1.31 q^{2/3} \quad \forall a \in F_q^*.$$ 

This bound is achieved by using only elementary tricks with character sums and no deep results from algebraic geometry are needed.

6. Power sums of Kloosterman sums over subfields

This section is not needed for the analysis of the cyclic codes but is just commenting the recent paper [4]. We count some power sums of Kloosterman sums over subfields. Here we relate (one-dimensional) Kloosterman sum over the extension field $F_{q^m}^*$

$$K^{(m)}(\alpha) = \sum_{x \in F_{q^m}^*} e(x + \alpha x^{-1}), \quad \alpha \in F_{q^m}^*,$$

to the (one-dimensional) Kloosterman sum over the subfield $F_q^*$

$$k_1(a) = \sum_{x \in F_q^*} \chi(x + ax^{-1}), \quad a \in F_q^*.$$

To that end we recall a proposition by Carlitz [2], or alternatively [9, Theorem 5.46]. This result holds for any $q = p^r$.

Proposition 15. With the above notation

$$K^{(m)}(a) = -D_m(-k_1(a), q) \quad \forall a \in F_q^*,$$

where $D_m(x, b)$ is the Dickson polynomial over integers.

For the properties of the Dickson polynomials we refer to [8]. For our studies it is enough to know that

$$D_2(x, b) = x^2 - 2b,$$
$$D_3(x, b) = x^3 - 3bx,$$
$$D_4(x, b) = x^4 - 4bx^2 + 2b^2,$$
and
$$D_6(x, b) = x^6 - 6bx^4 + 9b^2x^2 - 2b^3.$$ 

Remark 16. In [4] the authors pose an Open Problem which can be stated with our notation as: “Which values $K^{(2)}(a)$ takes for $a \in F_q^*$ when $q$ is even?” By the results of Carlitz [2] and Lachaud and Wolfmann [7] we already know that

$$\left\{ K^{(2)}(a) \mid a \in F_q^* \right\} = \left\{ 2q - i^2 \mid i \in [-2\sqrt{q}, 2\sqrt{q}], \quad i \equiv -1 \, (\text{mod} \, 4) \right\}.$$
More generally,
\[ \{ K^{(m)}(a) \mid a \in \mathbb{F}_q^* \} = \{-D_m(-i, q) \mid i \in [-2\sqrt{q}, 2\sqrt{q}], \ i \equiv -1 \ (\text{mod} \ 4)\}. \]

Next we count a sum from [4, Proposition 4] in a different way. That sum can be stated in the following equivalent form.

**Corollary 17.** If \( q \) is even, then
\[
\sum_{a \in \mathbb{F}_q^*} K^{(2)}(a)^2 = 4q + \sum_{a \in \mathbb{F}_q^*} k_1(a)^4 = 2q^3 - 2q^2 + q - 1.
\]

**Proof.** By Propositions 15 and 9 and Corollary 10 we have
\[
\sum_{a \in \mathbb{F}_q^*} K^{(2)}(a)^2 = \sum_{a \in \mathbb{F}_q^*} (k_1(a)^2 - 2q)^2 = \sum_{a \in \mathbb{F}_q^*} (k_1(a)^4 - 4qk_1(a)^2 + 4q^2)
\]
\[= 2q^3 - 2q^2 - 3q - 1 - 4q(q^2 - q - 1) + 4q^2(q - 1). \]

We generalize the previous result in two ways.

**Theorem 18.** If \( q = 2^r \), then
\[
\sum_{a \in \mathbb{F}_q^*} K^{(2)}(a)^3 = 3q^4 - 3q^3 + (-1)^r q^3 + 3q^2 - q + 1.
\]

**Proof.** By Proposition 15, Corollary 7, and the proof of Theorem 13 we have
\[
\sum_{a \in \mathbb{F}_q^*} K^{(2)}(a)^3 = \sum_{a \in \mathbb{F}_q^*} (2q - k_1(a))^3 = \sum_{a \in \mathbb{F}_q^*} (q - k_2(a))^3
\]
\[= \sum_{a \in \mathbb{F}_q^*} (q^3 - 3q^2k_2(a) + 3qk_2(a)^2 - k_2(a)^3)
\]
\[= q^3(q - 1) + 3q^2 + 3q(q^3 - q^2 - q - 1)
\]
\[= (q^4 - q^3 - (-1)^r q^3 - 3q^2 - 2q - 1). \]

**Theorem 19.** If \( q = 2^r \), then
\[
\sum_{a \in \mathbb{F}_q^*} K^{(3)}(a)^2 = 2q^4 - 2q^3 - (-1)^r q^3 + q - 1.
\]

**Proof.** By Proposition 15, Corollaries 7 and 10, and Theorem 18 we have
\[
\sum_{a \in \mathbb{F}_q^*} K^{(3)}(a)^2 = \sum_{a \in \mathbb{F}_q^*} k_1(a)^2 (k_1(a)^2 - 3q)^2 = \sum_{a \in \mathbb{F}_q^*} (k_2(a) + q)(k_2(a) - 2q)^2
\]
\[
= \sum_{a \in \mathbb{F}_q^*} (k_2(a)^3 - 3qk_2(a)^2 + 4q^3)
\]
\[
= (q^4 - q^3 - (-1)^r q^3 - 3q^2 - 2q - 1)
\]
\[
- 3q(q^3 - q^2 - q - 1) + 4q^3(q - 1).
\]

With the above results we can similarly count the following.

**Corollary 20.** If \( q = 2^r \), then
\[
\sum_{a \in \mathbb{F}_q^*} K^{(m)}(a) = \begin{cases} 
  q^2 - q + 1, & \text{if } m = 2; \\
  (-1)^r q^2 - q + 1, & \text{if } m = 3; \\
  -q + 1, & \text{if } m = 4; \\
  (-1)^r q^3 - q + 1, & \text{if } m = 6.
\end{cases}
\]

**Proof.** By Proposition 15 the task is to count power sums of \( k_1(a) \) and we know them by Proposition 9, Corollary 10, and Theorem 13.

7. **Codewords of weight 3 and 4 in \( C_{1,t} \)**

We consider the binary cyclic code \( C_{1,t} \) (see introduction) of length \( q^3 - 1 \) with \( q = 2^r \) and \( t = q^2 + q + 1 \). The dimension of this code equals \( q^3 - 1 - 4r \) because the 2-cyclotomic cosets modulo \( q^3 - 1 \) of 1 and \( t \) have orders \( 3r \) and \( r \), respectively.

We get the number of 3-weight codewords immediately from Theorem 5 and see that the minimum distance of \( C_{1,t} \) equals 3.

**Theorem 21.** The number of codewords of weight 3 in \( C_{1,t} \) is
\[
A_3 = (q^3 - 1) \frac{q^2 + (-1)^r q - 2}{6}.
\]

**Proof.** Codewords of weight 3 containing position 1 correspond to solutions \( x \in \mathbb{F}_{q^3} \setminus \{0, 1\} \) of equations
\[
\begin{cases} 
  1 + x + y = 0, \\
  1 + x^t + y^t = 0
\end{cases} \iff x^t + (1 + x)^t = 1.
\]

Clearly, 0 and 1 are solutions and by Theorem 5 we have \( q^2 + \chi(1)q - 2 = q^2 + (-1)^r q - 2 \) solutions \( x \in \mathbb{F}_{q^3} \setminus \{0, 1\} \).

The above codewords have \( q^3 - 1 \) cyclic shifts but counting them all gives every codeword 6 times.

**Remark 22.** With the results in [5] one can see, e.g., that for \( t = q^2 + q - 1 \) and \( t = q^2 - q + 1 \) the codes \( C_{1,t} \) have \( (q^3 - 1)(q^2 - 2)/6 \) and \( (q^3 - 1)(q - 2)/6 \) codewords of weight 3, respectively. In
these cases the key fact is that \( t \equiv 1 \pmod{q - 1} \). These results do not apply with \( t = q^2 + q + 1 \) as 1 and \( t \) do not belong to the same 2-cyclotomic coset modulo \( 2^3 - 1 \) or \( q - 1 \).

**Theorem 23.** The number of codewords of weight 4 in \( C_{1,t} \) is

\[
A_4 = \frac{q^3(q^3 - 1)(q^2 - 1)}{24} - A_3.
\]

**Proof.** We count a sum \( S = \sum_{\alpha, \beta \in \mathbb{F}_{q^3}} \left( \sum_{x \in \mathbb{F}_{q^3}} e(\alpha x^t + \beta x) \right)^4 \) in two ways. Firstly, by Proposition 4 and (3) we get

\[
S = \sum_{\beta \neq 0 \neq \alpha} (qk_1(N(\beta)\Tr(\alpha)^{-1}))^4 + \sum_{\alpha \in \mathbb{F}_{q^3}} \left( \sum_{x \in \mathbb{F}_{q^3}} e(\alpha x^t) \right)^4
\]

\[
= (q^5 - q^2)q^4 \sum_{\alpha \in \mathbb{F}_{q^2}} k_1(\alpha)^4 + \left[ q^2(q^3)^4 + (q^3 - q^2)(1 - \alpha)^4 \right]
\]

where \( \alpha \) can be chosen in \( q^3 - q^2 \) ways and \( \beta \) in \( t \) ways and together they give the factor \( q^5 - q^2 \). Altogether, by Corollary 10 we have \( S = q^9(q^5 + 2q^3 - q^2 - 1) \).

Secondly, the sum \( S \) is straightforwardly

\[
S = \sum_{x, y, z, w \in \mathbb{F}_{q^3}} \sum_{\alpha \in \mathbb{F}_{q^3}} e(\alpha(x^t + y^t + z^t + w^t)) \sum_{\beta \in \mathbb{F}_{q^3}} e(\beta(x + y + z + w))
\]

which equals \( q^6 \) times the number of solutions \((x, y, z, w) \in \mathbb{F}_{q^3}^4\) to the equations

\[
x + y + z + w = 0 \quad \& \quad x^t + y^t + z^t + w^t = 0.
\]

Indeed, if \((x, y, z, w) \in \mathbb{F}_{q^3}^4\) is a solution to the above equations, the inner sums in \( S \) equal \( q^3 \cdot q^3 \) by Lemma 2. On the other hand, if \((x, y, z, w) \in \mathbb{F}_{q^3}^4\) is not a solution, at least one of the inner sums equals zero by the same lemma.

In addition to codewords of weight 4 in \( C_{1,t} \) there are some extra solutions to the above equations. For example, if \( x = y \) then necessarily \( z = w \) and there are \( q^6 \) such solutions. There are also solutions with \( x = z \) or \( x = w \) but these solution sets intersect when \( x = y = z = w \). Therefore, there are \( 3q^6 - 2q^3 \) extra solutions to (4) such that the components are not pairwise distinct.

All in all, we have \((S/q^6 - (3q^6 - 2q^3))/24 = q^3(q^3 - 1)(q^2 - 1)/24 \) solutions with \( x < y < z < w \). Solutions with \( x = 0 \) correspond to codewords of weight 3 and this completes the proof. \( \square \)

8. Conclusions

We used relations of \( n \)-dimensional Kloosterman sums to exponential sums to count the number of codewords of weight 3 and 4 in a binary cyclic code \( C_{1,q^2+q+1} \) of length \( q^3 - 1 \). We suspect that something similar can be done in the case where \( t = (q^m - 1)/(q + 1) \) and \( m \) is
even. In the course of our study we counted some character sums explicitly and got also nice proof for an identity introduced by Carlitz. In addition, we were able to count some power sums of Kloosterman sums over subfields.

Question arises: Can one calculate the power sums of Kloosterman sums even further? Yes one can but the work of the first author [12], where some deep results from [13] are used, shows that the formulas for fifth, seventh, ninth, and every higher power sums will include number theoretic quantities like traces of Hecke operators and Ramanujan’s tau-function.

Acknowledgments

We thank the anonymous reviewers for valuable comments which improved this paper.

References