Simple Recursive Formulas Generating Power Moments of Kloosterman Sums

Dae San Kim

Department of Mathematics, Sogang University, Seoul 121-742, South Korea

Abstract

In this paper, we construct four binary linear codes closely connected with certain exponential sums over the finite field \( \mathbb{F}_q \) and \( \mathbb{F}_q - \{0, 1\} \). Here \( q \) is a power of two. Then we obtain four recursive formulas for the power moments of Kloosterman sums in terms of the frequencies of weights in the codes. This is done via Pless power moment identity and by utilizing the explicit expressions of the exponential sums obtained earlier.

Key words: recursive formula, Kloosterman sum, Pless power moment identity, weight distribution.

1 Introduction and Notations

Let \( \psi \) be a nontrivial additive character of the finite field \( \mathbb{F}_q \) with \( q = p^r \) elements (\( p \) a prime). Then the Kloosterman sum \( K(\psi; a) \) is defined as

\[
K(\psi; a) = \sum_{\alpha \in \mathbb{F}_q^*} \psi(\alpha + a\alpha^{-1})(a \in \mathbb{F}_q^*). 
\]

The Kloosterman sum was introduced in 1926 to give an estimate for the Fourier coefficients of modular forms. It has also been studied to solve various problems in coding theory and cryptography over finite fields of characteristic two.

---

1 This work was supported by grant No. R01-2006-000-11176-0 from the Basic Research Program of the Korea Science and Engineering Foundation.
2 Email address: dskim@sogang.ac.kr.
For each nonnegative integer \( h \), by \( MK(\psi)^h \) we will denote the \( h \)-th moment of the Kloosterman sum \( K(\psi; a) \). Namely, it is given by

\[
MK(\psi)^h = \sum_{a \in \mathbb{F}_q^*} K(\psi; a)^h.
\]

If \( \psi = \lambda \) is the canonical additive character of \( \mathbb{F}_q \), then \( MK(\lambda)^h \) will be simply denoted by \( MK^h \).

From now on, let us assume that \( q = 2^r \). Carlitz [1] evaluated \( MK^h \), for \( h \leq 4 \). Recently, Moisio was able to find explicit expressions of \( MK^h \), for the other values of \( h \) with \( h \leq 10 \) (cf. [6]). This was done, via Pless power moment identity, by connecting moments of Kloosterman sums and the frequencies of weights in the binary Zetterberg code of length \( q + 1 \), which were known by the work of Schoof and Vlugt in [7].

In this paper, we will produce four recursive formulas generating power moments of Kloosterman sums. To do that, we construct four binary linear codes closely connected with certain exponential sums (cf. Theorem 2). It is amusing that those exponential sums have been used repeatedly in our derivation of recursive formulas generating power moments of Kloosterman sums (cf. [3], [4]).

Theorem 1 of the following (cf. (1), (2), (4)-(9)) is the main result of this paper. Henceforth, we agree that the binomial coefficient \( \binom{b}{a} = 0 \), if \( a > b \) or \( a < 0 \).

**Theorem 1** Let \( q = 2^r \). Then we have the following.

(a) For \( r \geq 3 \), and \( h = 1, 2, \ldots \),

\[
MK^h = \sum_{l=0}^{h-1} (-1)^{h+l+1} \binom{h}{l} (q-1)^{h-l} MK^l
+ q \sum_{j=0}^{\min\{q-2, h\}} (-1)^{h+j} C_{1,j} \sum_{t=j}^{h} t! S(h, t) 2^{h-t} \binom{q-2-j}{q-2-t},
\]

where \( \{C_{1,j}\}_{j=0}^{q-2} \) is the weight distribution of the binary linear code \( C_1 \) given by

\[
C_{1,j} = \sum_{\text{tr}(\beta^{-1})=0} \prod_{\nu_\beta=0}^j \left( \binom{2}{\nu_\beta} \right) (j = 0, \ldots, q-2).
\]

Here the sum is over all the sets of nonnegative integers \( \{\nu_\beta\}_{\text{tr}(\beta^{-1})=0} \) satisfying \( \sum_{\text{tr}(\beta^{-1})=0} \nu_\beta = j \) and \( \sum_{\text{tr}(\beta^{-1})=0} \nu_\beta \beta = 0 \). In addition, \( S(h, t) \) is the Stirling number of the second kind defined by

\[
S(h, t) = \frac{1}{t!} \sum_{j=0}^{t} (-1)^{t-j} \binom{t}{j} j^h.
\]
(b) For \( r \geq 3 \), and \( h = 1, 2, \ldots \),

\[
MK^h = \sum_{l=0}^{h-1} (-1)^{h+l+1} \binom{h}{l} (q-1)^{h-l} MK^l
+ q \sum_{j=0}^{\min\left\{ \frac{q}{2}, h \right\}} (-1)^{h+j} C_{2,j} \sum_{t=0}^{h} t! S(h,t) 2^{2h-t} \left( \frac{q}{2} - 1 - j \right),
\]

(4)

where \( \{C_{2,j}\}_{j=0}^{q-1} \) is the weight distribution of the binary linear code \( C_2 \), and

\( C_{2,j}(0 \leq j \leq \frac{q}{2} - 1) \) is equal to the number of all the sets of nonnegative integers

\( \{\nu_\beta\}_{\text{tr}(\beta^{-1})=0} \) satisfying \( \nu_\beta = 0 \quad \text{or} \quad 1, \sum_{\text{tr}(\beta^{-1})=0} \nu_\beta = j \quad \text{and} \quad \sum_{\text{tr}(\beta^{-1})=0} \nu_\beta \beta = 0. \)

(5)

(c) For \( h = 1, 2, \ldots \),

\[
MK^h = - \sum_{l=0}^{h-1} \binom{h}{l} (q+1)^{h-l} MK^l
+ q \sum_{j=0}^{\min\{q, h\}} (-1)^j C_{3,j} \sum_{t=0}^{h} t! S(h,t) 2^{2h-t} \left( \frac{q}{2} - j \right),
\]

(6)

where \( \{C_{3,j}\}_{j=0}^{1} \) is the weight distribution of the binary linear code \( C_3 \) given by

\[
C_{3,j} = \sum_{\text{tr}(\beta^{-1})=1} \prod_{\nu_\beta} \left( \frac{2}{\nu_\beta} \right) (j = 0, \ldots, q).
\]

(7)

Here the sum is over all the sets of nonnegative integers \( \{\nu_\beta\}_{\text{tr}(\beta^{-1})=1} \) satisfying

\( \sum_{\text{tr}(\beta^{-1})=1} \nu_\beta = j \quad \text{and} \quad \sum_{\text{tr}(\beta^{-1})=1} \nu_\beta \beta = 0. \)

(d) For \( h = 1, 2, \ldots \),

\[
MK^h = - \sum_{l=0}^{h-1} \binom{h}{l} (q+1)^{h-l} MK^l
+ q \sum_{j=0}^{\min\{\frac{q}{2}, h\}} (-1)^j C_{4,j} \sum_{t=0}^{h} t! S(h,t) 2^{2h-t} \left( \frac{q}{2} - j \right),
\]

(8)

where \( \{C_{4,j}\}_{j=0}^{q/2} \) is the weight distribution of the binary linear code \( C_4 \), and

\( C_{4,j}(0 \leq j \leq \frac{q}{2}) \) is equal to the number of all the sets of nonnegative integers

\( \{\nu_\beta\}_{\text{tr}(\beta^{-1})=1} \) satisfying \( \nu_\beta = 0 \quad \text{or} \quad 1, \sum_{\text{tr}(\beta^{-1})=1} \nu_\beta = j \quad \text{and} \quad \sum_{\text{tr}(\beta^{-1})=1} \nu_\beta \beta = 0. \)

(9)
Before we proceed further, we will fix the notations that will be used throughout this paper:

\[ q = 2^r \ (r \in \mathbb{Z}_{>0}), \]

\[ \mathbb{F}_q = \text{the finite field with } q \text{ elements}, \]

\[ \text{tr}(x) = x + x^2 + \cdots + x^{2^r-1} \text{ the trace function } \mathbb{F}_q \rightarrow \mathbb{F}_2, \]

\[ \lambda(x) = (-1)^{\text{tr}(x)} \text{ the canonical additive character of } \mathbb{F}_q. \]

2 Two exponential sums

Let \( \mathbb{F}_2^+, \mathbb{F}_q^+ \) denote the additive groups of the fields \( \mathbb{F}_2, \mathbb{F}_q \), respectively. Then, with \( \Theta(x) = x^2 + x \) denoting the Artin-Schreier operator in characteristic two, we have the following exact sequence of groups:

\[ 0 \rightarrow \mathbb{F}_2^+ \rightarrow \mathbb{F}_q^+ \rightarrow \Theta(\mathbb{F}_q) \rightarrow 0. \]

Here the first map is the inclusion and the second is given by \( x \mapsto \Theta(x) = x^2 + x \). So

\[ \Theta(\mathbb{F}_q) = \{ \alpha^2 + \alpha \mid \alpha \in \mathbb{F}_q \}, \text{ and } [\mathbb{F}_q^+ : \Theta(\mathbb{F}_q)] = 2. \quad (10) \]

The next theorem is the key to the results of this paper.

**Theorem 2 ([2])** Let \( \lambda \) be the canonical additive character of \( \mathbb{F}_q \), and let \( a \in \mathbb{F}_q^* \). Then

\[ (a) \sum_{\alpha \in \mathbb{F}_q^* \setminus \{0,1\}} \lambda \left( \frac{a}{\alpha^2 + \alpha} \right) = K(\lambda; a) - 1, \]

\[ (b) \sum_{\alpha \in \mathbb{F}_q^*} \lambda \left( \frac{a}{\alpha^2 + \alpha + b} \right) = -K(\lambda; a) - 1, \text{ if } x^2 + x + b \in \mathbb{F}_q \text{ is irreducible over } \mathbb{F}_q, \]

or equivalently if \( b \in \mathbb{F}_q \setminus \Theta(\mathbb{F}_q) \text{(c.f.}(10)). \)

3 Construction of codes

Here we will construct four binary linear codes \( C_1 \) of length \( N_1 = q - 2(q \geq 4) \), \( C_2 \) of length \( N_2 = \frac{q}{2} - 1(q \geq 4) \), \( C_3 \) of length \( N_3 = q \), and \( C_4 \) of length \( N_4 = \frac{q}{2} \), which are closely connected with the exponential sums (a), (b) in Theorem 2.
Let $b \in \mathbb{F}_q \setminus \Theta(\mathbb{F}_q)$ be fixed, and let $\gamma_0 = 0, \gamma_1, \ldots, \gamma_{q^2-1}$ be a fixed ordering of the elements in $\Theta(\mathbb{F}_q) = \{\alpha^2 + \alpha \mid \alpha \in \mathbb{F}_q\}$. Then

$$\Theta(\mathbb{F}_q) = \{\gamma_0, \gamma_1, \ldots, \gamma_{q^2-1}\} = \{\beta \in \mathbb{F}_q \mid tr\beta = 0\},$$
$$b + \Theta(\mathbb{F}_q) = \{b + \gamma_0, b + \gamma_1, \ldots, b + \gamma_{q^2-1}\} = \{\beta \in \mathbb{F}_q \mid tr\beta = 1\},$$
$$\mathbb{F}_q = \{\gamma_0, \gamma_1, \ldots, \gamma_{q^2-1}\}.$$

Also, we put

$$v_1 = \left(\frac{1}{\gamma_1}, \frac{1}{\gamma_2}, \ldots, \frac{1}{\gamma_{q^2-1}}, \frac{1}{\gamma_1}, \frac{1}{\gamma_2}, \ldots, \frac{1}{\gamma_{q^2-1}}\right) \in \mathbb{F}_{N_1}^q,$$  \hspace{1cm} (11)
$$v_2 = \left(\frac{1}{\gamma_1}, \frac{1}{\gamma_2}, \ldots, \frac{1}{\gamma_{q^2-1}}\right) \in \mathbb{F}_{N_2}^q,$$  \hspace{1cm} (12)
$$v_3 = \left(\frac{1}{b + \gamma_0}, \frac{1}{b + \gamma_1}, \ldots, \frac{1}{b + \gamma_{q^2-1}}, \frac{1}{b + \gamma_0}, \frac{1}{b + \gamma_1}, \ldots, \frac{1}{b + \gamma_{q^2-1}}\right) \in \mathbb{F}_{N_3}^q,$$  \hspace{1cm} (13)
$$v_4 = \left(\frac{1}{b + \gamma_0}, \frac{1}{b + \gamma_1}, \ldots, \frac{1}{b + \gamma_{q^2-1}}\right) \in \mathbb{F}_{N_4}^q.$$  \hspace{1cm} (14)

**Remark 3** For each $i = 1, 2, 3, 4$, and each $\beta \in \mathbb{F}_q$, let $n_i(\beta)$ denote the number of components with those equal to $\beta$ in the vector $v_i$. Then it is obvious that

$$n_1(\beta) = \begin{cases} 2, & \text{if } \beta \in \mathbb{F}_q^* \text{, with } tr(\beta^{-1}) = 0, \\ 0, & \text{otherwise}, \end{cases}$$  \hspace{1cm} (15)
$$n_2(\beta) = \begin{cases} 1, & \text{if } \beta \in \mathbb{F}_q^* \text{, with } tr(\beta^{-1}) = 0, \\ 0, & \text{otherwise}, \end{cases}$$  \hspace{1cm} (16)
$$n_3(\beta) = \begin{cases} 2, & \text{if } tr(\beta^{-1}) = 1, \\ 0, & \text{otherwise}, \end{cases}$$  \hspace{1cm} (17)
$$n_4(\beta) = \begin{cases} 1, & \text{if } tr(\beta^{-1}) = 1, \\ 0, & \text{otherwise}. \end{cases}$$  \hspace{1cm} (18)

Then, for each $i = 1, 2, 3, 4$, the binary linear code $C_i$ is defined as

$$C_i = \{u \in \mathbb{F}_2^{N_i} \mid u \cdot v_i = 0\},$$  \hspace{1cm} (19)

where the dot denotes the usual inner product in $\mathbb{F}_{N_i}^q$.

The following Delsarte’s theorem is well-known.

**Theorem 4** ([5]) Let $B$ be a linear code over $\mathbb{F}_q$. Then

$$(B|\mathbb{F}_2)^\perp = tr(B^\perp).$$
In view of this theorem, the duals $C_i^\perp (i = 1, 2, 3, 4)$ are given by

$$C_1^\perp = \{ c_1(a) = \left( tr \frac{a}{\gamma_1}, tr \frac{a}{\gamma_2}, \ldots, tr \frac{a}{\gamma_{q^2-1}} \right) | a \in \mathbb{F}_q \},$$

(20)

$$C_2^\perp = \{ c_2(a) = \left( tr \frac{a}{\gamma_1}, tr \frac{a}{\gamma_2}, \ldots, tr \frac{a}{\gamma_{q^2-1}} \right) | a \in \mathbb{F}_q \},$$

(21)

$$C_3^\perp = \{ c_3(a) = \left( tr \frac{a}{b + \gamma_0}, \ldots, tr \frac{a}{b + \gamma_{q^2-1}}, tr \frac{a}{b + \gamma_0}, \ldots, tr \frac{a}{b + \gamma_{q^2-1}} \right) | a \in \mathbb{F}_q \},$$

(22)

$$C_4^\perp = \{ c_4(a) = \left( tr \frac{a}{b + \gamma_0}, tr \frac{a}{b + \gamma_1}, \ldots, tr \frac{a}{b + \gamma_{q^2-1}} \right) | a \in \mathbb{F}_q \}. \tag{23}$$

(a) and (b) can be respectively proved just as Theorem 11 in [3] and Theorem 13 in [4].

**Theorem 5** (a) For $q = 2^r$, with $r \geq 3$, the map $\mathbb{F}_q \rightarrow C_i^\perp (a \mapsto c_i(a))$, for $i = 1, 2$, is an $\mathbb{F}_2$-linear isomorphism.

(b) For every $q = 2^r$, the map $\mathbb{F}_q \rightarrow C_i^\perp (a \mapsto c_i(a))$, for $i = 3, 4$, is an $\mathbb{F}_2$-linear isomorphism.

**Remark 6** Note that, for $i = 1, 2$, and $q = 4$, the kernel of the map $\mathbb{F}_4 \rightarrow C_i^\perp (a \mapsto c_i(a))$ is $\mathbb{F}_2$.

4 Power moments of Kloosterman sums

In this section, we will be able to find, via Pless power moment identity, a recursive formula for the power moments of Kloosterman sums in terms of the frequencies of weights in $C_i$, for each $i = 1, 2, 3, 4$.

**Theorem 7 (Pless power moment identity)** Let $B$ be an $q$-ary $[n, k]$ code, and let $B_i$ (resp. $B_i^\perp$) denote the number of codewords of weight $i$ in $B$ (resp. in $B^\perp$). Then, for $h = 0, 1, 2, \ldots$,

$$\sum_{j=0}^{n} j^h B_j = \sum_{j=0}^{\min\{n,h\}} (-1)^j B_j \sum_{t=j}^{h} t! S(h, t) q^{k-t}(q-1)^{t-j} \binom{n-j}{n-t}, \quad (24)$$

where $S(h, t)$ is the Stirling number of the second kind defined in (4).

**Lemma 8** For $i = 1, 2, 3, 4$, and $a \in \mathbb{F}_q^*$, the Hamming weight $w(c_i(a))$ (cf.
(20)-(23)) can be expressed as follows:

(a) \( w(c_1(a)) = \frac{1}{2}(q - 1 - K(\lambda; a)) \),

(b) \( w(c_2(a)) = \frac{1}{4}(q - 1 - K(\lambda; a)) \),

(c) \( w(c_3(a)) = \frac{1}{2}(q + 1 + K(\lambda; a)) \),

(d) \( w(c_4(a)) = \frac{1}{4}(q + 1 + K(\lambda; a)) \).

**Proof.** We will just show (c) and (d), as (a) and (b) can be proved in a similar manner.

\[
w(c_3(a)) = \frac{1}{2} \cdot 2 \cdot \sum_{j=0}^{2^{q-1}} (1 - (-1)^{tr(\frac{a}{b+\gamma_j})})(cf. (22))
\]

\[
= \frac{1}{2}(q - 2 \sum_{j=0}^{2^{q-1}} \lambda(\frac{a}{b+\gamma_j}))
\]

\[
= \frac{1}{2}(q - \sum_{a \in \mathbb{F}_q} \lambda(\frac{a}{\alpha^2 + \alpha + b}))
\]

\[
= \frac{1}{2}(q - (-K(\lambda; a) - 1)).(by \, \text{Theorem} \, 2 \, \text{(b)})
\]

Further, we see that \( w(c_4(a)) = \frac{1}{2} w(c_3(a)) \). \( \square \)

Denote for the moment \( v_i \) in (11)-(14) by \( v_i = (g_1, g_2, \ldots, g_{N_i}) \), for \( i = 1, 2, 3, 4 \).

Fix \( i(i = 1, 2, 3, 4) \), and let \( u = (u_1, \ldots, u_{N_i}) \in \mathbb{F}_q^{N_i} \), with \( \nu_\beta \) 1’s in the coordinate places where \( g_i = \beta \), for each \( \beta \in \mathbb{F}_q \). Then we see from the definition of the code \( C_i \)(cf. (19)) that \( u \) is a codeword with weight \( j \) if and only if \( \sum_{\beta \in \mathbb{F}_q} \nu_\beta = j \) and \( \sum_{\beta \in \mathbb{F}_q} \nu_\beta \beta = 0 \)(an identity in \( \mathbb{F}_q \)). As there are \( \prod_{\beta \in \mathbb{F}_q} \left( \binom{n(\beta)}{\nu_\beta} \right) \)(cf. Remark 3) many such codewords with weight \( j \), we obtain the following result.

**Proposition 9** Let \( \{C_{i,j}\}_{j=0}^{N_i} \) be the weight distribution of \( C_i \), for each \( i = 1, 2, 3, 4 \), where \( C_{i,j} \) denotes the frequency of the codewords with weight \( j \) in \( C_i \). Then

\[
C_{i,j} = \sum \prod_{\beta \in \mathbb{F}_q} \left( \binom{n(\beta)}{\nu_\beta} \right),
\]

where the sum runs over all the sets of integers \( \{\nu_\beta\}_{\beta \in \mathbb{F}_q} \) (0 \( \leq \nu_\beta \leq n(\beta) \)), satisfying

\[
\sum_{\beta \in \mathbb{F}_q} \nu_\beta = j, \, \text{and} \, \sum_{\beta \in \mathbb{F}_q} \nu_\beta \beta = 0.
\]
Corollary 10 Let \( \{C_{i,j}\}_{j=0}^{N_i} \) be the weight distribution of \( C_i \), for \( i = 1, 3 \). Then we have \( C_{i,j} = C_{i,N_i-j} \), for all \( j \), with \( 0 \leq j \leq N_i \).

**Proof.** Under the replacements \( \nu_\beta \rightarrow n_i(\beta) - \nu_\beta \), for each \( \beta \in \mathbb{F}_q \), the first equation in (30) is changed to \( N_i - j \), while the second one in (30) and the summands in (29) are left unchanged. Here the second sum in (30) is left unchanged, since \( \sum_{\beta \in \mathbb{F}_q} n_i(\beta) = 0 \), for \( i = 1, 3 \) (cf. (15), (17)). □

Now, we get the formulas in (2), (5), (7), and (9), by applying the formula in (29) to each \( C_i \), using the values of \( n_i(\beta) \) in (15)-(18).

From now on, we will assume that \( r \geq 3 \), for \( i = 1, 2 \), and hence, for \( i = 1, 2, 3, 4 \), every codeword in \( C_i^\perp \) can be written as \( c_i(a) \), for a unique \( a \in \mathbb{F}_q \) (cf. Theorem 5). Then we apply the Pless power moment identity in (24) to each \( C_i^\perp \), for \( i = 1, 2, 3, 4 \), in order to obtain the results in Theorem 1(cf. (1), (2), (4)-(9)) about recursive formulas. Then the left hand side of that identity in (24) is equal to

\[
\sum_{a \in \mathbb{F}_q^*} w(c_i(a))^h,
\]

with the \( w(c_i(a)) \) in each case given by (25)-(28).

**References**

[1] L. Carlitz, “Gauss sums over finite fields of order \( 2^n \),” Acta Arith. vol.15, pp. 247-265, 1969.

[2] D.S.Kim, “Codes associated with special linear groups and power moments of multi-dimensional Kloosterman sums,” submitted.

[3] D.S.Kim, “Codes associated with \( O^+(2n,2^r) \) and power moments of Kloosterman sums,” submitted.

[4] D.S.Kim, “Codes associated with \( O^-(2n,2^r) \) and power moments of Kloosterman sums,” submitted.

[5] F. J. MacWilliams and N. J. A. Sloane, “The Theory of Error Correcting Codes,” Amsterdam, The Netherlands: North-Holland, 1998.

[6] M. Moisio, “The moments of a Kloosterman sum and the weight distribution of a Zetterberg-type binary cyclic code,” IEEE Trans. Inform. Theory, vol. 53, pp. 843-847, 2007.

[7] R. Schoof and M. van der Vlugt, “Hecke operators and the weight distributions of certain codes,” J. Combin. Theory Ser. A, vol. 57, pp. 163-186, 1991.