Recursive formulas generating power moments of multi-dimensional Kloosterman sums and m-multiple power moments of Kloosterman sums*

Dae San Kim

Communicated by V. V. Kirichenko

ABSTRACT. In this paper, we construct two binary linear codes associated with multi-dimensional and $m-$multiple power Kloosterman sums (for any fixed m) over the finite field $\mathbb{F}_q$. Here q is a power of two. The former codes are dual to a subcode of the binary hyper-Kloosterman code. Then we obtain two recursive formulas for the power moments of multi-dimensional Kloosterman sums and for the m-multiple power moments of Kloosterman sums in terms of the frequencies of weights in the respective codes. This is done via Pless power moment identity and yields, in the case of power moments of multi-dimensional Kloosterman sums, much simpler recursive formulas than those associated with finite special linear groups obtained previously.

1. Introduction and Notations

Let ψ be a nontrivial additive character of the finite field $\mathbb{F}_q$ with $q = p^r$ elements (p a prime), and let m be a positive integer. Then the

m-dimensional Kloosterman sum $K_m(\psi; a)$([10]) is defined by

$$K_m(\psi; a) = \sum_{\alpha_1, \cdots, \alpha_m \in \mathbb{F}_q^*} \psi(\alpha_1 + \cdots + \alpha_m + a\alpha_1^{-1} \cdots \alpha_m^{-1}) \ (a \in \mathbb{F}_q^*).$$

For this, we have the Deligne bound

$$|K_m(\psi; a)| \leqslant (m+1)q^{\frac{m}{2}}. \tag{1.1}$$

In particular, if $m = 1$, then $K_1(\psi; a)$ is simply denoted by $K(\psi; a)$, and is called the Kloosterman sum. The Kloosterman sum was introduced in 1926 [8] 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.

For each nonnegative integer h, we denote by $MK_m(\psi)^h$ the h-th moment of the m-dimensional Kloosterman sum $K_m(\psi; a)$, i.e.,

$$MK_m(\psi)^h = \sum_{a \in \mathbb{F}_q^*} K_m(\psi; a)^h.$$

If $\psi = \lambda$ is the canonical additive character of $\mathbb{F}_q$, then $MK_m(\lambda)^h$ will be simply denoted by MK_m^h. If futher $m = 1$, for brevity MK_1^h will be indicated by MK^h. The power moments of Kloosterman sums can be used, for example, to give an estimate for the Kloosterman sums.

Explicit computations on power moments of Kloosterman sums were initiated in the paper [17] of Salié in 1931, where it is shown that for any odd prime q,

$$MK^h = q^2 M_{h-1} - (q-1)^{h-1} + 2(-1)^{h-1} \quad (h \geqslant 1).$$

Here $M_0 = 0$, and, for $h \in \mathbb{Z}_{>0}$,

$$M_h = |\{(\alpha_1, \cdots, \alpha_h) \in (\mathbb{F}_q^*)^h | \sum_{j=1}^{h} \alpha_i = 1 = \sum_{j=1}^{h} \alpha_i^{-1}\}|.$$

For $q = p$ an odd prime, Salié obtained MK^1, MK^2, MK^3, MK^4 in that same paper by determining M_1, M_2, M_3. On the other hand, MK^5 can be expressed in terms of the p-th eigenvalue for a weight 3 newform on $\Gamma_0(15)$ (cf. [11], [16]). MK^6 can be expressed in terms of the p-th eigenvalue for a weight 4 newform on $\Gamma_0(6)$ (cf.[4]). Also, based on numerical evidence, in [3] Evans was led to propose a conjecture which

expresses MK^7 in terms of Hecke eigenvalues for a weight 3 newform on $\Gamma_0(525)$ with quartic nebentypus of conductor 105.

From now on, let us assume that $q = 2^r$. Carlitz [1] evaluated MK^h for $h \leqslant 4$. Recently, Moisio was able to find explicit expressions of MK^h, for $h \leqslant 10$ (cf. [13]). 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 [18].

Also, Moisio considered binary hyper-Kloosterman codes $C(r, m)$ and determined the weight distributions of $C(r, m)$ and $C^{\perp}(r, m)$, for $r = 2$ and all $m \geqslant 2$, and for all $r \geqslant 2$ and $m = 3$ (cf. [14]). In [15], these results were further extended to the case of $r = 3, 4$ and all $m \geqslant 2$.

In this paper, we construct two binary linear codes C_{n-1} and D_m, respectively connected with multi-dimensional and m-multiple power Kloosterman sums (for any fixed m) over the finite field $\mathbb{F}_q$. Here q is a power of two. The code $C_{n-1}^{\perp}$ is a subcode of the hyper-Kloosterman code $C(r, n)$, which is mentioned above. Then we obtain two recursive formulas for the power moments of multi-dimensional Kloosterman sums and the m-multiple power moments of Kloosterman sums in terms of the frequencies of weights in the respective codes. This is done via Pless power moment identity and yields, in the case of power moments of multi-dimensional Kloosterman sums, much simpler recursive formulas than those obtained previously in [5]. As for the case of q a power of three, in [6] two infinite families of ternary linear codes associated with double cosets in the symplectic group $Sp(2n, q)$ were constructed in order to generate infinite families of recursive formulas for the power moments of Kloosterman sums with square arguments and for the even power moments of those in terms of the frequencies of weights in those codes.

Theorem 1.1. (1) *Let $n = 2^s$, $q = 2^r$. For $r \geqslant 3$, and $h = 1, 2, \cdots$,*

$$MK_{n-1}^h = \sum_{l=0}^{h-1}(-1)^{h+l+1}\binom{h}{l}(q-1)^{(n-1)(h-l)}MK_{n-1}^l$$

$$+ q \sum_{j=0}^{\min\{(q-1)^{n-1},\, h\}}(-1)^{h+j}C_{n-1,j}\sum_{t=j}^{h}t!S(h,t)2^{h-t}\binom{(q-1)^{n-1}-j}{(q-1)^{n-1}-t}. \quad (1.2)$$

Here $S(h, t)$ indicates the Stirling number of the second kind given by

$$S(h, t) = \frac{1}{t!}\sum_{j=0}^{t}(-1)^{t-j}\binom{t}{j}j^h. \quad (1.3)$$

In addition, $\{C_{n-1,j}\}_{j=0}^{(q-1)^{n-1}}$ denotes the weight distribution of the binary linear code C_{n-1}, given by

$$C_{n-1,j} = \sum \prod_{\beta \in \mathbb{F}_q} \binom{\delta(n-1,q;\beta)}{\nu_\beta}, \qquad (1.4)$$

where the sum runs over all the sets of integers $\{\nu_\beta\}_{\beta \in \mathbb{F}_q} (0 \leqslant \nu_\beta \leqslant \delta(n-1,q;\beta))$ satisfying

$$\sum_{\beta \in \mathbb{F}_q} \nu_\beta = j, \qquad \sum_{\beta \in \mathbb{F}_q} \nu_\beta \beta = 0 \qquad (1.5)$$

and $\delta(n-1,q;\beta) = |\{(\alpha_1, \cdots, \alpha_{n-1}) \in (\mathbb{F}_q^*)^{n-1}|$

$$\alpha_1 + \cdots + \alpha_{n-1} + \alpha_1^{-1} \cdots \alpha_{n-1}^{-1} = \beta\}|$$

$$= \begin{cases} q^{-1}\{(q-1)^{n-1} + 1\}, & \text{if } \beta = 0, \\ K_{n-2}(\lambda; \beta^{-1}) + q^{-1}\{(q-1)^{n-1} + 1\}, & \text{if } \beta \in \mathbb{F}_q^*. \end{cases}$$

Here we understand that $K_0(\lambda; \beta^{-1}) = \lambda(\beta^{-1})$.

(2) Let $q = 2^r$. For $r \geqslant 3$, and $m, h = 1, 2, \cdots$,

$$MK^{mh} = \sum_{l=0}^{h-1} (-1)^{h+l+1} \binom{h}{l} (q-1)^{m(h-l)} MK^{ml}$$
$$+ q \sum_{j=0}^{\min\{(q-1)^m, h\}} (-1)^{h+j} D_{m,j} \sum_{t=j}^{h} t! S(h,t) 2^{h-t} \binom{(q-1)^m - j}{(q-1)^m - t}. \qquad (1.6)$$

Here $\{D_{m,j}\}_{j=0}^{(q-1)^m}$ is the weight distribution of the binary linear code D_m, given by

$$D_{m,j} = \sum \prod_{\beta \in \mathbb{F}_q} \binom{\sigma(m,q;\beta)}{\nu_\beta}, \qquad (1.7)$$

where the sum runs over all the sets of integers $\{\nu_\beta\}_{\beta \in \mathbb{F}_q} (0 \leqslant \nu_\beta \leqslant \sigma(m,q;\beta))$ satisfying (1.5), and

$$\sigma(m,q;\beta) = |\{(\alpha_1, \cdots, \alpha_m) \in (\mathbb{F}_q^*)^m|$$
$$\alpha_1 + \cdots + \alpha_m + \alpha_1^{-1} + \cdots + \alpha_m^{-1} = \beta\}| \qquad (1.8)$$
$$= \sum \lambda(\alpha_1 + \cdots + \alpha_m) + q^{-1}\{(q-1)^m + (-1)^{m+1}\},$$

with the sum running over all $\alpha_1, \cdots, \alpha_m \in \mathbb{F}_q^*$, satisfying $\alpha_1^{-1} + \cdots + \alpha_m^{-1} = \beta$.

(1) and (2) of the following are respectively $n = 2$ and $n = 4$ cases of Theorem 1.1 (1) (cf. (3.3), (3.4)), and (3) and (4) are equivalent and $n = 2$ case of Theorem 1.1 (2) ((cf. (5.4), (5.8)).

Corollary 1.2. (1) *Let* $q = 2^r$. *For* $r \geqslant 3$, *and* $h = 1, 2, \cdots$,

$$
\begin{aligned}
MK^h &= \sum_{l=0}^{h-1} (-1)^{h+l+1} \binom{h}{l} (q-1)^{h-l} MK^l \\
&\quad + q \sum_{j=0}^{\min\{(q-1),h\}} (-1)^{h+j} C_{1,j} \sum_{t=j}^{h} t! S(h,t) 2^{h-t} \binom{q-1-j}{q-1-t},
\end{aligned}
\tag{1.9}
$$

where $\{C_{1,j}\}_{j=0}^{q-1}$ *is the weight distribution of the binary linear code* C_1, *with*

$$
C_{1,j} = \sum \binom{1}{\nu_0} \prod_{\mathrm{tr}(\beta^{-1})=0} \binom{2}{\nu_\beta} \quad (j = 0, \cdots, N_1).
$$

Here the sum is over all the sets of nonnegative integers $\{\nu_0\} \bigcup \{\nu_\beta\}_{\mathrm{tr}(\beta^{-1})=0}$ *satisfying* $\nu_0 + \sum_{\mathrm{tr}(\beta^{-1})=0} \nu_\beta = j$ *and* $\sum_{\mathrm{tr}(\beta^{-1})=0} \nu_\beta \beta = 0$.
   (2) *Let* $q = 2^r$. *For* $r \geqslant 3$, *and* $h = 1, 2, \cdots$,

$$
\begin{aligned}
MK_3^h &= \sum_{l=0}^{h-1} (-1)^{h+l+1} \binom{h}{l} (q-1)^{3(h-l)} MK_3^l \\
&\quad + q \sum_{j=0}^{min\{(q-1)^3,h\}} (-1)^{h+j} C_{3,j} \sum_{t=j}^{h} t! S(h,t) 2^{h-t} \binom{(q-1)^3-j}{(q-1)^3-t},
\end{aligned}
\tag{1.10}
$$

where $\{C_{3,j}\}_{j=0}^{(q-1)^3}$ *is the weight distribution of the binary linear code* C_3, *with*

$$
C_{3,j} = \sum \binom{m_0}{\nu_0} \prod_{\substack{|t|<2\sqrt{q} \\ t \equiv -1(4)}} \prod_{K(\lambda;\beta^{-1})=t} \binom{m_t}{\nu_\beta}.
$$

Here the sum runs over all the sets of nonnegative integers $\{\nu_\beta\}_{\beta \in \mathbb{F}_q}$ *satisfying* (1.5),

$$
m_0 = q^2 - 3q + 3,
$$

and

$$
m_t = t^2 + q^2 - 4q + 3,
$$

for every integer t satisfying $|t| < 2\sqrt{q}$ and $t \equiv -1(4)$.
    (3) Let $q = 2^r$. For $r \geqslant 3$, and $h = 1, 2, \cdots$,

$$MK^{2h} = \sum_{l=0}^{h-1}(-1)^{h+l+1}\binom{h}{l}(q-1)^{2(h-l)}MK^{2l}$$
$$+ q \sum_{j=0}^{\min\{(q-1)^2,h\}}(-1)^{h+j}D_{2,j}\sum_{t=j}^{h}t!S(h,t)2^{h-t}\binom{(q-1)^2-j}{(q-1)^2-t},$$
(1.11)

where $\{D_{2,j}\}_{j=0}^{(q-1)^2}$ is the weight distribution of the binary linear code D_2, with

$$D_{2,j} = \sum\binom{2q-3}{\nu_0}\prod_{\beta\in\mathbb{F}_q^*}\binom{K(\lambda;\beta^{-1})+q-3}{\nu_\beta}$$
$$= \sum\binom{2q-3}{\nu_0}\prod_{\substack{|t|<2\sqrt{q} \\ t\equiv-1(4)}}\prod_{K(\lambda;\beta^{-1})=t}\binom{t+q-3}{\nu_\beta},$$
(1.12)

with the sum running over all the sets of nonnegative integers $\{\nu_\beta\}_{\beta\in\mathbb{F}_q}$ satisfying (1.5).
    (4) Let $q = 2^r$. For $r \geqslant 3$, and $h = 1, 2, \cdots$,

$$MK_2^h = \sum_{l=0}^{h-1}(-1)^{h+l+1}\binom{h}{l}(q^2-3q+1)^{(h-l)}MK_2^l$$
$$+ q \sum_{j=0}^{\min\{(q-1)^2,h\}}(-1)^{h+j}D_{2,j}\sum_{t=j}^{h}t!S(h,t)2^{h-t}\binom{(q-1)^2-j}{(q-1)^2-t},$$
(1.13)

where $D_{2,j}(0 \leqslant j \leqslant (q-1)^2)$'s are just as in (1.12).

The next two theorems will be of use later.

Theorem 1.3 ([9]). *Let $q = 2^r$, with $r \geqslant 2$. Then the range R of $K(\lambda; a)$, as a varies over $\mathbb{F}_q^*$, is given by*

$$R = \{t \in \mathbb{Z} \mid |t| < 2\sqrt{q}, \ t \equiv -1(mod4)\}.$$

In addition, each value $t \in R$ is attained exactly $H(t^2 - q)$ times, where $H(d)$ is the Kronecker class number of d.

Theorem 1.4 ([2]). *For the canonical additive character λ of $\mathbb{F}_q$, and $a \in \mathbb{F}_q^*$,*

$$K_2(\lambda; a) = K(\lambda; a)^2 - q. \qquad (1.14)$$

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

$$q = 2^r \ (r \in \mathbb{Z}_{>0}),$$
$$\mathbb{F}_q = the \ finite \ field \ with \ q \ elements,$$
$$\mathrm{tr}(x) = x + x^2 + \cdots + x^{2^{r-1}} \ the \ trace \ function \ \mathbb{F}_q \ \to \ \mathbb{F}_2,$$
$$\lambda(x) = (-1)^{\mathrm{tr}(x)} \ the \ canonical \ additive \ character \ of \ \mathbb{F}_q.$$

Note that any nontrivial additive character ψ of $\mathbb{F}_q$ is given by $\psi(x) = \lambda(ax)$, for a unique $a \in \mathbb{F}_q^*$.

2.   Construction of codes associated with multi-dimensional Kloosterman sums

We will construct binary linear codes C_{n-1} of length $N_1 = (q-1)^{n-1}$, connected with the $(n-1)$-dimensional Kloosterman sums. Here $n = 2^s$, with $s \in \mathbb{Z}_{>0}$.

Let

$$v_{n-1} = (\cdots, \alpha_1 + \cdots + \alpha_{n-1} + \alpha_1^{-1} \cdots \alpha_{n-1}^{-1}, \cdots), \qquad (2.1)$$

where $\alpha_1, \alpha_2, \cdots, \alpha_{n-1}$ run respectively over all elements of $\mathbb{F}_q^*$. Here we do not specify the ordering of the components of v_{n-1}, but we assume that some ordering is fixed.

Proposition 2.1 ([5], Proposition 11). *For each $\beta \in \mathbb{F}_q$, let*

$$\delta(n-1, q; \beta)$$
$$= |\{(\alpha_1, \cdots, \alpha_{n-1}) \in (\mathbb{F}_q^*)^{n-1} | \alpha_1 + \cdots, +\alpha_{n-1} + \alpha_1^{-1} \cdots \alpha_{n-1}^{-1} = \beta\}|$$

(Note that $\delta(n-1, q; \beta)$ is the number of components with those equal to β in the vector $v_{n-1}(cf.(2.1))$). Then

$$\delta(n-1, q; 0) = q^{-1}\{(q-1)^{n-1} + 1\},$$

and, for $\beta \in \mathbb{F}_q^*$,

$$\delta(n-1, q; \beta) = K_{n-2}(\lambda; \beta^{-1}) + q^{-1}\{(q-1)^{n-1} + 1\},$$

where $K_0(\lambda; \beta^{-1}) = \lambda(\beta^{-1})$ by convention.

Corollary 2.2.

$$(1) \quad \delta(1, q; \beta) = \begin{cases} 2, & \text{if } \operatorname{tr}(\beta^{-1}) = 0, \\ 1, & \text{if } \beta = 0, \\ 0, & \text{if } \operatorname{tr}(\beta^{-1}) = 1. \end{cases} \tag{2.2}$$

$$(2) \quad \delta(3, q; \beta) = \begin{cases} q^2 - 3q + 3, & \text{if } \beta = 0, \\ K(\lambda; \beta^{-1})^2 + q^2 - 4q + 3, & \text{if } \beta \in \mathbb{F}_q^* \ (cf.(1.14)). \end{cases} \tag{2.3}$$

The binary linear code C_{n-1} is defined as

$$C_{n-1} = \{u \in \mathbb{F}_2^{N_1} | u \cdot v_{n-1} = 0\}, \tag{2.4}$$

where the dot denotes the usual inner product in $\mathbb{F}_q^{N_1}$.

The following Delsarte's theorem is well-known.

Theorem 2.3 ([12]). *Let B be a linear code over $\mathbb{F}_q$. Then*

$$(B|_{\mathbb{F}_2})^{\perp} = \operatorname{tr}(B^{\perp}).$$

In view of this theorem, the dual $C_{n-1}^{\perp}$ of C_{n-1} is given by

$$C_{n-1}^{\perp} = \{c(a) = (\cdots, \operatorname{tr}(a(\alpha_1 + \cdots + \alpha_{n-1} + \alpha_1^{-1} \cdots \alpha_{n-1}^{-1})), \cdots) | a \in \mathbb{F}_q\}. \tag{2.5}$$

Lemma 2.4. $(q-1)^{n-1} > nq^{\frac{n-1}{2}}$, *for all $n = 2^s$ ($s \in \mathbb{Z}_{>0}$), and $q = 2^r \geqslant 8$.*

Proof. This can be proved, for example, by induction on s. $\qquad\square$

Proposition 2.5. *For $q = 2^r$, with $r \geqslant 3$, the map $\mathbb{F}_q \to C_{n-1}^{\perp}(a \mapsto c(a))$ is an $\mathbb{F}_2$-linear isomorphism.*

Proof. The map is clearly $\mathbb{F}_2$-linear and onto. Let a be in the kernel of the map. Then $\operatorname{tr}(a(\alpha_1 + \cdots + \alpha_{n-1} + \alpha_1^{-1} \cdots \alpha_{n-1}^{-1})) = 0$, for all $\alpha_1, \cdots, \alpha_{n-1} \in \mathbb{F}_q^*$. Suppose that $a \neq 0$. Then, on the one hand,

$$\sum_{\alpha_1, \cdots, \alpha_{n-1} \in \mathbb{F}_q^*} (-1)^{\operatorname{tr}(a(\alpha_1 + \cdots + \alpha_{n-1} + \alpha_1^{-1} \cdots \alpha_{n-1}^{-1}))} = (q-1)^{n-1} = N_1. \tag{2.6}$$

On the other hand, (2.6) is equal to $K_{n-1}(\lambda; a)$ (cf. proof of Proposition 11 in [5]), and so from Deligne's estimate in (1.1) we get

$$(q-1)^{n-1} \leqslant nq^{\frac{n-1}{2}}.$$

But this is impossible for $q \geqslant 8$, in view of Lemma 2.4. $\qquad\square$

3. Recursive formulas for power moments
   of multi-dimensional Kloostermann sums

We are now ready to derive, via Pless power moment identity, a recursive formula for the power moments of multi-dimensional Kloosterman sums in terms of the frequencies of weights in C_{n-1}.

Theorem 3.1 (Pless power moment identity, [12])**.** *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 $h = 0,1,2,\cdots$,*

$$\sum_{i=0}^{n} i^h B_i = \sum_{i=0}^{\min\{n,h\}} (-1)^i B_i^\perp \sum_{t=i}^{h} t! S(h,t) q^{k-t}(q-1)^{t-i} \binom{n-i}{n-t}, \quad (3.1)$$

where $S(h,t)$ is the Stirling number of the second kind defined in(1.3).

For the following lemma, observe that $(n, q-1) = 1$.

Lemma 3.2. *The map $a \mapsto a^n : \mathbb{F}_q^* \to \mathbb{F}_q^*$ is a bijection.*

Lemma 3.3. *For $a \in \mathbb{F}_q^*$, the Hamming weight $w(c(a))(cf.\ (2.5))$ of $c(a)$ can be expressed as follows:*

$$w(c(a)) = \frac{N_1}{2} - \frac{1}{2} K_{n-1}(\lambda; a), \ with \ N_1 = (q-1)^{n-1}. \qquad (3.2)$$

Proof.

$$w(c(a)) = \frac{1}{2} \sum_{\alpha_1,\cdots,\alpha_{n-1}\in\mathbb{F}_q^*} (1 - (-1)^{\operatorname{tr}(a(\alpha_1+\cdots+\alpha_{n-1}+\alpha_1^{-1}\cdots\alpha_{n-1}^{-1}))})$$

$$= \frac{1}{2}\{N_1 - \sum_{\alpha_1,\cdots,\alpha_{n-1}\in\mathbb{F}_q^*} \lambda(a(\alpha_1+\cdots+\alpha_{n-1}+\alpha_1^{-1}\cdots\alpha_{n-1}^{-1}))\}$$

$$= \frac{N_1}{2} - \frac{1}{2} \sum_{\alpha_1,\cdots,\alpha_{n-1}\in\mathbb{F}_q^*} \lambda(\alpha_1+\cdots+\alpha_{n-1}+a^n\alpha_1^{-1}\cdots\alpha_{n-1}^{-1})$$

$$= \frac{N_1}{2} - \frac{1}{2} \sum_{\alpha_1,\cdots,\alpha_{n-1}\in\mathbb{F}_q^*} \lambda(\alpha_1^n+\cdots+\alpha_{n-1}^n+a^n\alpha_1^{-n}\cdots\alpha_{n-1}^{-n})$$

(by Lemma 3.2)

$$= \frac{N_1}{2} - \frac{1}{2} \sum_{\alpha_1,\cdots,\alpha_{n-1}\in\mathbb{F}_q^*} \lambda((\alpha_1+\cdots+\alpha_{n-1}+a\alpha_1^{-1}\cdots\alpha_{n-1}^{-1})^n)$$

$$= \frac{N_1}{2} - \frac{1}{2} \sum_{\alpha_1,\cdots,\alpha_{n-1}\in\mathbb{F}_q^*} \lambda(\alpha_1+\cdots+\alpha_{n-1}+a\alpha_1^{-1}\cdots\alpha_{n-1}^{-1})$$

([10], Theorem 2.23(v))

$$= \frac{N_1}{2} - \frac{1}{2} K_{n-1}(\lambda; a). \qquad \square$$

Denote for the moment v_{n-1} in (2.1) by $v_{n-1} = (g_1, g_2, \cdots, g_{N_1})$. Let $u = (u_1, \cdots, u_{N_1}) \in \mathbb{F}_2^{N_1}$, with ν_β 1's in the coordinate places where $g_l = \beta$, for each $\beta \in \mathbb{F}_q$. Then we see from the definition of the code C_{n-1} (cf. (2.4)) 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 $\prod_{\beta \in \mathbb{F}_q} \binom{\delta(n-1,q;\beta)}{\nu_\beta}$ (cf. Proposition 2.1) many such codewords with weight j, we obtain the following result.

Proposition 3.4. *Let* $\{C_{n-1,j}\}_{j=0}^{N_1}$ *be the weight distribution of* C_{n-1}, *where* $C_{n-1,j}$ *denotes the frequency of the codewords with weight* j *in* C_{n-1}. *Then*

$$C_{n-1,j} = \sum \prod_{\beta \in \mathbb{F}_q} \binom{\delta(n-1,q;\beta)}{\nu_\beta},$$

where the sum runs over all the sets of integers $\{\nu_\beta\}_{\beta \in \mathbb{F}_q}$ ($0 \leqslant \nu_\beta \leqslant \delta(n-1,q;\beta)$) *satisfying*

$$\sum_{\beta \in \mathbb{F}_q} \nu_\beta = j, \text{ and } \sum_{\beta \in \mathbb{F}_q} \nu_\beta \beta = 0.$$

Corollary 3.5. (1) *Let* $\{C_{1,j}\}_{j=0}^{q-1}$ *be the weight distribution of* C_1. *Then*

$$C_{1,j} = \sum \binom{1}{\nu_0} \prod_{\mathrm{tr}(\beta^{-1})=0} \binom{2}{\nu_\beta} \quad (j = 0, \cdots, q-1), \qquad (3.3)$$

where the sum is over all the sets of nonnegative integers $\{\nu_0\} \cup \{\nu_\beta\}_{\mathrm{tr}(\beta^{-1})=0}$ *satisfying* $\nu_0 + \sum_{\mathrm{tr}(\beta^{-1})=0} \nu_\beta = j$ *and* $\sum_{\mathrm{tr}(\beta^{-1})=0} \nu_\beta \beta = 0$ *(cf.(2.2))*.

(2) *Let* $\{C_{3,j}\}_{j=0}^{(q-1)^3}$ *be the weight distribution of* C_3. *Then*

$$C_{3,j} = \sum \binom{m_0}{\nu_0} \prod_{\substack{|t|<2\sqrt{q} \\ t \equiv -1(4)}} \prod_{K(\lambda;\beta^{-1})=t} \binom{m_t}{\nu_\beta}, \qquad (3.4)$$

where the sum runs over all the sets of integers $\{\nu_\beta\}_{\beta \in \mathbb{F}_q}$ *satisfying*

$$\sum_{\beta \in \mathbb{F}_q} \nu_\beta = j, \text{ and } \sum_{\beta \in \mathbb{F}_q} \nu_\beta \beta = 0,$$

$$m_0 = q^2 - 3q + 3,$$

and

$$m_t = t^2 + q^2 - 4q + 3,$$

for every integer t satisfying $|t| < 2\sqrt{q}$ and $t \equiv -1(4)$ (cf. Theorem 1.3, (2.3)).

Remark 3.6. This shows that the weight distribution of C_1 is the same as that of $C(SO^+(2,q))$ (cf. [7]).

From now on, we will assume that $r \geqslant 3$, and hence every codeword in $C_{n-1}^\perp$ can be written as $c(a)$, for a unique $a \in \mathbb{F}_q$ (cf. Proposition 2.5).

We now apply the Pless power moment identity in (3.1) to $C_{n-1}^\perp$, in order to obtain the result in Theorem 1.1 (1) about a recursive formula. Then the left hand side of that identity in (3.1) is equal to

$$\sum_{a \in \mathbb{F}_q^*} w(c(a))^h, \tag{3.5}$$

with $w(c(a))$ given by (3.2). So (3.5) is

$$\sum_{a \in \mathbb{F}_q^*} w(c(a))^h = \frac{1}{2^h} \sum_{a \in \mathbb{F}_q^*} (N_1 - K_{n-1}(\lambda; a))^h$$

$$= \frac{1}{2^h} \sum_{a \in \mathbb{F}_q^*} \sum_{l=0}^h (-1)^l \binom{h}{l} N_1^{h-1} K_{n-1}(\lambda; a)^l \tag{3.6}$$

$$= \frac{1}{2^h} \sum_{l=0}^h (-1)^l \binom{h}{l} N_1^{h-1} MK_{n-1}^l.$$

On the other hand, noting that $dim_{\mathbb{F}_2} C_{n-1} = r$ (cf. Proposition 2.5) the right hand side of the Pless moment identity(cf. (3.1)) becomes

$$q \sum_{j=0}^{\min\{N_1,h\}} (-1)^j C_{n-1,j} \sum_{t=j}^h t! S(h,t) 2^{-t} \binom{N_1 - j}{N_1 - t}. \tag{3.7}$$

Our result in (1.2) follows now by equating (3.6) and (3.7).

Remark 3.7. A recursive formula for the power moments of multi-dimensional Kloosterman sums was obtained in [5] by constructing binary linear codes $C(SL(n,q))$ and utilizing explicit expressions of Gauss sums for the finite special linear group $SL(n,q)$. However, our result in (1.2) is better than that in (1) of [5]. Because our formula here is much simpler than the one there. Indeed, the length of the code C_{n-1} here is $N_1 = (q-1)^{n-1}$, whereas that of $C(SL(n,q))$ there is $N = q^{\binom{n}{2}} \prod_{j=2}^n (q^j - 1)$, both of which appear in their respective expressions of recursive formulas.

4. Construction of codes associated with powers of Kloosterman sums

We will construct binary linear codes D_m of length $N_2 = (q-1)^m$, connected with the m-th powers of (the ordinary) Kloosterman sums. Here $m \in \mathbb{Z}_{>0}$.

Let

$$w_m = (\cdots, \alpha_1 + \cdots + \alpha_m + \alpha_1^{-1} + \cdots + \alpha_m^{-1}, \cdots), \qquad (4.1)$$

where $\alpha_1, \alpha_2, \cdots, \alpha_m$ run respectively over all elements of $\mathbb{F}_q^*$. Here we do not specify the ordering of the components of w_m, but we assume that some ordering is fixed.

Theorem 4.1 ([7]). *Let λ be the canonical additive character of $\mathbb{F}_q$, and let $\beta \in \mathbb{F}_q^*$. Then*

$$\sum_{\alpha \in \mathbb{F}_q - \{0,1\}} \lambda(\frac{\beta}{\alpha^2 + \alpha}) = K(\lambda; \beta) - 1. \qquad (4.2)$$

Proposition 4.2. *For each $\beta \in \mathbb{F}_q$, let*

$$\sigma(m, q; \beta) = |\{(\alpha_1, \cdots, \alpha_m) \in (\mathbb{F}_q^*)^m | \alpha_1 + \cdots + \alpha_m + \alpha_1^{-1} + \cdots + \alpha_m^{-1} = \beta\}|$$

(Note that $\sigma(m, q; \beta)$ is the number of components with those equal to β in the vector w_m (cf. (4.1)). Then

$$(1) \quad \sigma(m, q; \beta) = \sum \lambda(\alpha_1 + \cdots + \alpha_m) + q^{-1}\{(q-1)^m + (-1)^{m+1}\}, \quad (4.3)$$

where the sum in (4.3) runs over all $\alpha_1, \cdots, \alpha_m \in \mathbb{F}_q^*$, satisfying $\alpha_1^{-1} + \cdots + \alpha_m^{-1} = \beta$.

$$(2) \quad \sigma(2, q; \beta) = \begin{cases} 2q - 3, & \text{if } \beta = 0, \\ K(\lambda; \beta^{-1}) + q - 3, & \text{if } \beta \neq 0. \end{cases} \qquad (4.4)$$

Proof. (1) can be proved just as Proposition 2.1(cf. [5], Proposition 11). The details are left to the reader.

(2) If $m = 2$, from (4.3)

$$\sigma(2, q; \beta) = \sum \lambda(\alpha_1 + \alpha_2) + q - 2, \qquad (4.5)$$

where α_1 and α_2 run over all elements in $\mathbb{F}_q^*$, satisfying $\alpha_1^{-1} + \alpha_2^{-1} = \beta$.

If $\beta = 0$, then the result is clear. Assume now that $\beta \neq 0$. Then the sum in (4.5) is

$$\sum_{\alpha_1 \in \mathbb{F}_q - \{0, \beta^{-1}\}} \lambda(\alpha_1 + (\alpha_1^{-1} + \beta)^{-1})$$

$$= \sum_{\alpha_1 \in \mathbb{F}_q - \{0, \beta\}} \lambda(\alpha_1^{-1} + (\alpha_1 + \beta)^{-1}) \quad (\alpha_1 \to \alpha_1^{-1})$$

$$= \sum_{\alpha_1 \in \mathbb{F}_q - \{0, 1\}} \lambda(\frac{\beta^{-1}}{\alpha_1^2 + \alpha_1}) \quad (\alpha_1 \to \beta\alpha_1)$$

$$= K(\lambda; \beta^{-1}) - 1 \ (cf.(4.2)). \qquad \square$$

The binary linear code D_m is defined as

$$D_m = \{u \in \mathbb{F}_2^{N_2} | u \cdot w_m = 0\},$$

where the dot denotes the usual inner product in $\mathbb{F}_q^{N_2}$.

Remark 4.3. Clearly, the binary linear codes C_1 and D_1 coincide.

In view of Theorem 2.3, the dual $D_m^\perp$ of D_m is given by

$$D_m^\perp = \{d(a) = (\cdots, \mathrm{tr}(a(\alpha_1 + \cdots + \alpha_m + \alpha_1^{-1} + \cdots + \alpha_m^{-1})), \cdots) | a \in \mathbb{F}_q\}. \tag{4.6}$$

Lemma 4.4. $(q-1)^m > 2^m q^{\frac{m}{2}}$, for all $m \in \mathbb{Z}_{>0}$ and $q = 2^r \geqslant 8$.

Proof. This can be shown, for example, by induction on m. $\qquad \square$

Proposition 4.5. *For $q = 2^r$, with $r \geqslant 3$, the map $\mathbb{F}_q \to D_m^\perp (a \mapsto d(a))$ is an $\mathbb{F}_2$-linear isomorphism.*

Proof. The map is clearly $\mathbb{F}_2$-linear and onto. Let a be in the kernel of the map. Then $\mathrm{tr}(a(\alpha_1 + \cdots + \alpha_m + \alpha_1^{-1} + \cdots + \alpha_m^{-1})) = 0$, for all $\alpha_1, \cdots, \alpha_m \in \mathbb{F}_q^*$. Suppose that $a \neq 0$. Then, on the one hand,

$$\sum_{\alpha_1, \cdots, \alpha_m \in \mathbb{F}_q^*} (-1)^{\mathrm{tr}(a(\alpha_1 + \cdots + \alpha_m + \alpha_1^{-1} + \cdots + \alpha_m^{-1}))} = (q-1)^m = N_2. \tag{4.7}$$

On the other hand, (4.7) is equal to $K(\lambda; a)^m$, and so from Weil's estimate (i.e. (1.1) with $m = 1$) we get

$$(q-1)^m \leqslant 2^m q^{\frac{m}{2}}.$$

But this is impossible for $q \geqslant 8$, in view of Lemma 4.4. $\qquad \square$

5. Recursive formulas for *m*-multiple power moments of Kloostermann sums

We are now ready to derive, via Pless power moment identity, a recursive formula for the *m*-multiple power moments of Kloosterman sums in terms of the frequencies of weights in D_m.

Lemma 5.1. *For $a \in \mathbb{F}_q^*$, the Hamming weight $w(d(a))$ of $d(a)$ (cf. (4.6)) can be expressed as follows:*

$$w(d(a)) = \frac{N_2}{2} - \frac{1}{2}K(\lambda; a)^m, \; \text{with } N_2 = (q-1)^m. \tag{5.1}$$

Proof. This can be shown exactly as the proof of Lemma 3.3. □

Corollary 5.2. *For $m = 2$,*

$$w(d(a)) = \frac{1}{2}(q^2 - 3q + 1 - K_2(\lambda; a)) \; (cf.(1.14)). \tag{5.2}$$

The same argument leading to Proposition 3.4 shows the next proposition.

Proposition 5.3. *Let $\{D_{m,j}\}_{j=0}^{N_2}$ be the weight distribution of D_m, where $D_{m,j}$ denotes the frequency of the codewords with weight j in D_m. Then*

$$D_{m,j} = \sum \prod_{\beta \in \mathbb{F}_q} \binom{\sigma(m, q; \beta)}{\nu_\beta}, \tag{5.3}$$

where the sum runs over all the sets of integers $\{\nu_\beta\}_{\beta \in \mathbb{F}_q}$ ($0 \leqslant \nu_\beta \leqslant \sigma(m, q; \beta)$), satisfying

$$\sum_{\beta \in \mathbb{F}_q} \nu_\beta = j, \; and \; \sum_{\beta \in \mathbb{F}_q} \nu_\beta \beta = 0.$$

Corollary 5.4. *Let $\{D_{2,j}\}_{j=0}^{(q-1)^2}$ be the weight distribution of D_2, and let $q = 2^r$, with $r \geqslant 2$. Then, in view of Theorem 1.3 and (4.4), we have*

$$D_{2,j} = \sum \binom{2q - 3}{\nu_0} \prod_{\beta \in \mathbb{F}_q^*} \binom{K(\lambda; \beta^{-1}) + q - 3}{\nu_\beta}$$

$$= \sum \binom{2q - 3}{\nu_0} \prod_{\substack{|t| < 2\sqrt{q} \\ t \equiv -1(4)}} \prod_{K(\lambda;\beta^{-1})=t} \binom{t + q - 3}{\nu_\beta}, \tag{5.4}$$

where the sum runs over all the sets of nonnegative integers $\{\nu_\beta\}_{\beta \in \mathbb{F}_q}$
satisfying

$$\sum_{\beta \in \mathbb{F}_q} \nu_\beta = j \quad and \quad \sum_{\beta \in \mathbb{F}_q} \nu_\beta \beta = 0.$$

From now on, we will assume that $r \geqslant 3$, *and hence every codeword*
in $D_m^\perp$ *can be written as* $d(a)$, *for a unique* $a \in \mathbb{F}_q$(*cf. Proposition 4.5*).

We now apply the Pless power moment identity in (3.1) to $D_m^\perp$, in
order to obtain the result in Theorem 1.1 (1) about a recursive formula.
Then the left hand side of that identity in (3.1) is equal to

$$\sum_{a \in \mathbb{F}_q^*} w(d(a))^h, \tag{5.5}$$

with $w(d(a))$ given by (5.1). So (5.5) is seen to be equal to

$$\sum_{a \in \mathbb{F}_q^*} w(d(a))^h = \frac{1}{2^h} \sum_{l=0}^{h} (-1)^l \binom{h}{l} N_2^{h-l} M K^{ml}. \tag{5.6}$$

On the other hand, noting that $dim_{\mathbb{F}_2} D_m = r$(cf. Proposition 4.5) the
right hand side of the Pless moment identity(cf. (3.1)) becomes

$$q \sum_{j=0}^{\min\{N_2,h\}} (-1)^j D_{m,j} \sum_{t=j}^{h} t! S(h,t) 2^{-t} \binom{N_2 - j}{N_2 - t}. \tag{5.7}$$

Our result in (1.6) follows now by equating (5.6) and (5.7).

Remark 5.5. If $m = 2$, from the alternative expression of $w(d(a))$ in (5.2)
we see that (5.5) can also be given as

$$\sum_{a \in \mathbb{F}_q^*} w(d(a))^h = \frac{1}{2^h} \sum_{l=0}^{h} (-1)^l \binom{h}{l} (q^2 - 3q + 1)^{h-l} M K_2^l. \tag{5.8}$$

References

[1] L. Carlitz, *Gauss sums over finite fields of order* 2^n, Acta. Arith. **15**(1969), 247–265.

[2] L. Carlitz, *A note on exponential sums*, Pacific J. Math. **30**(1969), 35–37.

[3] R. J. Evans, *Seventh power moments of Kloosterman sums*, Israel J. Math. **175**(2010), 349–362.

[4] K. Hulek, J. Spandaw, B. van Geemen, and D. van Straten, *The modularity of the Barth-Nieto quintic and its relatives*, Adv. Geom. **1**(2001), 263-289.

[5] D. S. Kim, *Codes associated with special linear groups and power moments of multi-dimensional Kloosterman sums,* Ann. Mat. Pura Appli. **190**(2011), 61-76.

[6] D. S. Kim, *Infinite families of recursive formulas generating power moments of ternary Kloosterman sums with square arguments arising from symplectic groups,* Adv. Math. Commun. **3**(2009), 167–178.

[7] D. S. Kim, *Codes associated with $O^+(2n, 2^r)$ and power moments of Kloosterman sums*, Integers **12**(2012), 237–257.

[8] H. D. Kloosterman, *On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$*, Acta Math. **49**(1926), 407-464.

[9] G. Lachaud and J. Wolfmann, *The weights of the orthogonals of the extended quadratic binary Goppa codes*, IEEE Trans. Inform. Theory **36**(1990), 686-692.

[10] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl.**20**, Cambridge University Pless, Cambridge, 1987.

[11] R. Livné, *Motivic orthogonal two-dimensional representations of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$*, Israel J. Math. **92**(1995), 149-156.

[12] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, North-Holland, Amsterdam, 1998.

[13] M. Moisio, *The moments of a Kloosterman sum and the weight distribution of a Zetterberg-type binary cyclic code*, IEEE Trans. Inform. Theory **53**(2007), 843-847.

[14] M. Moisio, *On the duals of binary hyper-Kloosterman codes*, SIAM J. Disc. Math. **22**(2008), 273-287.

[15] M. Moisio, K. Ranto, M. Rinta-aho and Väänänen, *On the weight distribution of the duals of irreducible cyclic codes, cyclic codes with two zeros and hyper-Kloosterman codes*, Adv. Appl. Discrete Math. **3**(2009), 155-164.

[16] C. Peters, J. Top, and M. van der Vlugt, *The Hasse zeta function of a K3 surface related to the number of words of weight 5 in the Melas codes*, J. Reine Angew. Math. **432**(1992), 151-176.

[17] H. Salié, *Über die Kloostermanschen Summen $\mathcal{S}(u, v; q)$*, Math. Z. **34**(1931), 91-109.

[18] R. Schoof and M. van der Vlugt, *Hecke operators and the weight distributions of certain codes*, J. Combin. Theory Ser. A **57**(1991), 163-186.

Contact information

Dae San Kim   Department of Mathematics, Sogang University, Seoul 121-742, South Korea
E-Mail(s): dskim@sogang.ac.kr