J. Korean Math. Soc. **57** (2020), No. 3, pp. 585–602
https://doi.org/10.4134/JKMS.j190225
pISSN: 0304-9914 / eISSN: 2234-3008

CONSTRUCTION OF RECURSIVE FORMULAS GENERATING POWER MOMENTS OF KLOOSTERMAN SUMS: $O^+(2n, 2^r)$ CASE

Dae San Kim

Abstract. In this paper, we construct four infinite families of binary linear codes associated with double cosets with respect to a certain maximal parabolic subgroup of the orthogonal group $O^+(2n, 2^r)$. And we obtain two infinite families of recursive formulas for the power moments of Kloosterman sums and those of 2-dimensional 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 exponential sums over those double cosets related to the evaluations of "Gauss sums" for the orthogonal groups $O^+(2n, 2^r)$.

1. Introduction

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 $K_m(\psi; a)$ ([15]) is defined by

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

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 to give an estimate for the Fourier coefficients of modular forms (cf. [4,13]). It has also been studied to solve various problems in coding theory and cryptography over finite fields of characteristic two (cf. [3, 5]).

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.,

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

Received March 18, 2019; Accepted June 26, 2019.

2010 *Mathematics Subject Classification.* 11T23, 20G40, 94B05.

Key words and phrases. Kloosterman sum, 2-dimensional Kloosterman sum, orthogonal group, double cosets, maximal parabolic.

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 further $m = 1$, for brevity MK_1^h will be indicated by MK^h.

Explicit computations on power moments of Kloosterman sums were initiated in the paper [20] of Salié in 1931, where it is shown that, for any odd prime q,

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

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

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

For $q = p$ an odd prime, Salié obtained MK^1, MK^2, MK^3, MK^4 in [20] by determining M_1, M_2, M_3. MK^5 can be expressed in terms of the p-th eigenvalue of a weight 3 newform on $\Gamma_0(15)$ (cf. [16,19]). MK^6 can be expressed in terms of the p-th eigenvalue of a weight 4 newform on $\Gamma_0(6)$ (cf. [7]). In [6], Evans was led to propose a conjecture which expresses MK^7 in terms of Hecke eigenvalues of 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 $h \leq 4$. Recently, Moisio was able to find explicit expressions of MK^h, for the other values of h with $h \leq 10$ (cf. [18]). 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 [21].

In [10], the binary linear codes $C(SL(n, q))$ associated with finite special linear groups $SL(n, q)$ were constructed when n, q are both powers of two. Then we obtained a recursive formula for the power moments of multi-dimensional Kloosterman sums in terms of the frequencies of weights in $C(SL(n, q))$.

In this paper, we will be able to produce two infinite families of recursive formulas generating power moments of Kloosterman sums and two those of 2-dimensional Kloosterman sums. To do that, we construct four infinite families of binary linear codes $C(DC_1^+(n, q))$ $(n = 2, 4, \ldots)$, $C(DC_1^-(n, q))$ $(n = 1, 3, \ldots)$, both associated with $P^+\sigma_{n-1}^+P^+$, and $C(DC_2^+(n, q))$ $(n = 2, 4, \ldots)$, $C(DC_2^-(n, q))$ $(n = 3, 5, \ldots)$, both associated with $P^+\sigma_{n-2}^+P^+$, with respect to the maximal parabolic subgroup $P^+ = P^+(2n, q)$ of the orthogonal group $O^+(2n, q)$, and express those power moments in terms of the frequencies of weights in each code. Then, thanks to our previous results on the explicit expressions of exponential sums over those double cosets related to the evaluations of "Gauss sums" for the orthogonal groups $O^+(2n, q)$ [12], we can express the weight of each codeword in the duals of the codes in terms of Kloosterman or 2-dimensional Kloosterman sums. Then our formulas will follow immediately from the Pless' power moment identity. Analogously to these, in [9], for q a power of three, 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. We emphasize here that there have been only a few recursive formulas generating power moments of Kloosterman sums including the one in [18].

Theorem 1.1 in the following (cf. (9), (10), (12)-(14)) is the main result of this paper. To simplify notations, we introduce the following ones which will be used throughout this paper at various places.

$$A_1^{+}(n,q) = q^{\frac{1}{4}(5n^2-6n)} \left[\begin{smallmatrix} n \\ 1 \end{smallmatrix}\right]_q \prod_{j=1}^{n/2}(q^{2j-1}-1), \tag{1}$$

$$B_1^{+}(n,q) = q^{\frac{1}{4}(n-2)^2} \prod_{j=1}^{n/2}(q^{2j}-1), \tag{2}$$

$$A_2^{+}(n,q) = q^{\frac{1}{4}(5n^2-6n)} \left[\begin{smallmatrix} n \\ 2 \end{smallmatrix}\right]_q \prod_{j=1}^{(n-2)/2}(q^{2j-1}-1), \tag{3}$$

$$B_2^{+}(n,q) = q^{\frac{1}{4}(n^2-8n+12)}(q^{n-1}-1)(q^n-1) \prod_{j=1}^{(n-2)/2}(q^{2j}-1), \tag{4}$$

$$A_1^{-}(n,q) = q^{\frac{1}{4}(5n^2-4n-1)} \left[\begin{smallmatrix} n \\ 1 \end{smallmatrix}\right]_q \prod_{j=1}^{(n-1)/2}(q^{2j-1}-1), \tag{5}$$

$$B_1^{-}(n,q) = q^{\frac{1}{4}(n^2-6n+5)}(q^n-1) \prod_{j=1}^{(n-1)/2}(q^{2j}-1), \tag{6}$$

$$A_2^{-}(n,q) = q^{\frac{1}{4}(5n^2-8n+3)} \left[\begin{smallmatrix} n \\ 2 \end{smallmatrix}\right]_q \prod_{j=1}^{(n-1)/2}(q^{2j-1}-1), \tag{7}$$

$$B_2^{-}(n,q) = q^{\frac{1}{4}(n-3)^2}(q^n-1) \prod_{j=1}^{(n-1)/2}(q^{2j}-1). \tag{8}$$

From now on, it is assumed that either $+$ signs or $-$ signs are chosen everywhere, whenever $\pm$ signs appear. Henceforth we agree that the binomial coefficient $\binom{b}{a} = 0$, if $a > b$ or $a < 0$.

Theorem 1.1. *Let $q = 2^r$. Then, with the notations in* (1)-(8), *we have the following.*

(a) *With + signs everywhere for ± signs, we have a recursive formula generating power moments of Kloosterman sums over $\mathbb{F}_q$, for each $n \geq 2$ even and all q. Also, with − signs everywhere for ± signs, we have such a formula, for either each $n \geq 3$ odd and all q, or $n = 1$ and $q \geq 8$:*

$$\begin{aligned} MK^h = & \sum_{l=0}^{h-1} (-1)^{h+l+1} \binom{h}{l} B_1^{\pm}(n,q)^{h-l} MK^l \\ & + qA_1^{\pm}(n,q)^{-h} \sum_{j=0}^{\min\{N_1^{\pm}(n,q),h\}} (-1)^{h+j} C_{1,j}^{\pm}(n,q) \\ & \sum_{t=j}^{h} t! S(h,t) 2^{h-t} \binom{N_1^{\pm}(n,q)-j}{N_1^{\pm}(n,q)-t} \quad (h = 1, 2, \ldots), \end{aligned} \tag{9}$$

where $N_1^{\pm}(n,q) = |DC_1^{\pm}(n,q)| = A_1^{\pm}(n,q)B_1^{\pm}(n,q)$, and $\{C_{1,j}^{\pm}(n,q)\}_{j=0}^{N_1^{\pm}(n,q)}$ is the weight distribution of $C(DC_1^{\pm}(n,q))$ given by

$$\begin{aligned} C_{1,j}^{\pm}(n,q) = & \sum \binom{q^{-1}A_1^{\pm}(n,q)(B_1^{\pm}(n,q)+1)}{\nu_0} \\ & \times \prod_{tr(\beta^{-1})=0} \binom{q^{-1}A_1^{\pm}(n,q)(B_1^{\pm}(n,q)+q+1)}{\nu_\beta} \\ & \times \prod_{tr(\beta^{-1})=1} \binom{q^{-1}A_1^{\pm}(n,q)(B_1^{\pm}(n,q)-q+1)}{\nu_\beta}. \end{aligned} \tag{10}$$

Here the sum is over all the sets of nonnegative integers $\{\nu_\beta\}_{\beta \in \mathbb{F}_q}$ satisfying $\sum_{\beta \in \mathbb{F}_q} \nu_\beta = j$ and $\sum_{\beta \in \mathbb{F}_q} \nu_\beta \beta = 0$. In addition, $S(h,t)$ is the Stirling number of the second kind defined by

$$S(h,t) = \frac{1}{t!} \sum_{j=0}^{t} (-1)^{t-j} \binom{t}{j} j^h. \tag{11}$$

(b) *With + signs everywhere for ± signs, we have recursive formulas generating power moments of 2-dimensional Kloosterman sums over $\mathbb{F}_q$ and even power moments of Kloosterman sums over $\mathbb{F}_q$, for each even $n \geq 2$ and all $q \geq 4$. Also, with − signs everywhere for ± signs, we have such formulas, for each $n \geq 3$ odd and $q \geq 4$:*

$$MK_2^h = \sum_{l=0}^{h-1} (-1)^{h+l+1} \binom{h}{l} (B_2^{\pm}(n,q) - q^2)^{h-l} MK_2^l$$

$$+\,qA_2^{\pm}(n,q)^{-h}\sum_{j=0}^{\min\{N_2^{\pm}(n,q),h\}}(-1)^{h+j}C_{2,j}^{\pm}(n,q) \tag{12}$$
$$\sum_{t=j}^{h}t!S(h,t)2^{h-t}\binom{N_2^{\pm}(n,q)-j}{N_2^{\pm}(n,q)-t}\quad (h=1,2,\ldots),$$

and

$$MK^{2h}=\sum_{l=0}^{h-1}(-1)^{h+l+1}\binom{h}{l}(B_2^{\pm}(n,q)-q^2+q)^{h-l}MK^{2l}$$
$$+\,qA_2^{\pm}(n,q)^{-h}\sum_{j=0}^{\min\{N_2^{\pm}(n,q),h\}}(-1)^{h+j}C_{2,j}^{\pm}(n,q) \tag{13}$$
$$\sum_{t=j}^{h}t!S(h,t)2^{h-t}\binom{N_2^{\pm}(n,q)-j}{N_2^{\pm}(n,q)-t}\quad (h=1,2,\ldots),$$

where $N_2^{\pm}(n,q)=|DC_2^{\pm}(n,q)|=A_2^{\pm}(n,q)B_2^{\pm}(n,q)$, *and* $\{C_{2,j}^{\pm}(n,q)\}_{j=0}^{N_2^{\pm}(n,q)}$ *is the weight distribution of* $C(DC_2^{\pm}(n,q))$ *given by*

$$C_{2,j}^{\pm}(n,q)=\sum\binom{q^{-1}A_2^{\pm}(n,q)(B_2^{\pm}(n,q)+q^3-q^2-1)}{\nu_0}$$
$$\times\prod_{\substack{|\tau|<2\sqrt{q}\\ \tau\equiv-1(4)}}\ \prod_{K(\lambda;\beta^{-1})=\tau}\binom{q^{-1}A_2^{\pm}(n,q)(B_2^{\pm}(n,q)+q\tau-q^2-1)}{\nu_\beta}. \tag{14}$$

Here the sum is over all the sets of nonnegative integers $\{\nu_\beta\}_{\beta\in\mathbb{F}_q}$ *satisfying* $\sum_{\beta\in\mathbb{F}_q}\nu_\beta=j$, *and* $\sum_{\beta\in\mathbb{F}_q}\nu_\beta\beta=0$.

The following corollary is just the $n=2$ and $n=1$ cases of (a) in the above. It is amusing to note that the recursive formula in (15) and (16), obtained from the binary code $C(DC_1^{-}(1,q))$ associated with the double coset $DC_1^{-}(1,q)=P^{+}(2,q)$, is the same as the one in ([5], (1), (2)), gotten from the binary code $C(SO^{+}(2,q))$ associated with the special orthogonal group $SO^{+}(2,q)$.

Corollary 1.2. (a) *For all q, and $h = 1, 2, \ldots,$*

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

where $\{C_{1,j}^{+}(2,q)\}_{j=0}^{q^2(q^2-1)^2}$ is the weight distribution of $C(DC_1^{+}(2,q))$ given by

$$\begin{aligned} C_{1,j}^{+}(2,q) = \sum \binom{q^3(q^2-1)}{\nu_0} & \prod_{tr(\beta^{-1})=0} \binom{q^2(q-1)(q+1)^2}{\nu_\beta} \\ & \times \prod_{tr(\beta^{-1})=1} \binom{q^2(q+1)(q-1)^2}{\nu_\beta}. \end{aligned}$$

Here the sum is over all the sets of nonnegative integers $\{\nu_\beta\}_{\beta \in \mathbb{F}_q}$ satisfying $\sum_{\beta \in \mathbb{F}_q} \nu_\beta = j$ and $\sum_{\beta \in \mathbb{F}_q} \nu_\beta \beta = 0$. In addition, $S(h,t)$ is the Stirling number of the second kind as defined in (11).

(b) *Let $q \geq 8$. For $h = 1, 2, \ldots,$*

$$\begin{aligned} MK^h = & \sum_{l=0}^{h-1} (-1)^{h+l+1} \binom{h}{l} (q-1)^{h-l} MK^l \\ & + q \sum_{j=0}^{\min\{q-1, h\}} (-1)^{h+j} C_{1,j}^{-}(1,q) \sum_{t=j}^{h} t! S(h,t) 2^{h-t} \binom{q-1-j}{q-1-t}, \end{aligned} \tag{15}$$

where $\{C_{1,j}^{-}(1,q)\}_{j=0}^{q-1}$ is the weight distribution of $C(DC_1^{-}(n,q))$ given by

$$C_{1,j}^{-}(n,q) = \sum \binom{1}{\nu_0} \prod_{tr(\beta^{-1})=0} \binom{2}{\nu_\beta}. \tag{16}$$

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

2. $O^{+}(2n, q)$

For more details about this section, the reader is referred to the paper [12]. Throughout this paper, the following notations will be used:

$q = 2^r$ $(r \in \mathbb{Z}_{>0})$,
$\mathbb{F}_q$ = the finite field with q elements,
TrA = the trace of A for a square matrix A,
${}^tB$ = the transpose of B for any matrix B.

Let θ^+ be the nondegenerate quadratic form on the vector space $\mathbb{F}_q^{2n\times 1}$ of all $2n \times 1$ column vectors over $\mathbb{F}_q$, given by

$$\theta^+(\sum_{i=1}^{2n} x_i e^i) = \sum_{i=1}^{n} x_i x_{n+i},$$

where $\{e^1 =^t [10\dots0], e^2 =^t [010\dots0], \dots, e^{2n} =^t [0\dots01]\}$ is the standard basis of $\mathbb{F}_q^{2n\times 1}$.

The group $O^+(2n,q)$ of all isometries of $(\mathbb{F}_q^{2n\times 1},\ \theta^+)$ is given by:

$$O^+(2n,q) = \left\{ \left[\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right] \in GL(2n,q) \middle| \begin{smallmatrix} {}^tAC,\ {}^tBD \text{ are alternating} \\ {}^tAD+{}^tCB=1_n \end{smallmatrix} \right\}$$

$$= \left\{ \left[\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right] \in GL(2n,q) \middle| \begin{smallmatrix} {}^tAB,\ {}^tCD\text{are alternating} \\ A\ {}^tD+B\ {}^tC=1_n \end{smallmatrix} \right\},$$

where A, B, C, D are of size n.

Here an $n \times n$ matrix (a_{ij}) is called alternating if

$$\begin{cases} a_{ii} = 0 & \text{for } 1 \le i \le n, \\ a_{ij} = -a_{ji} = a_{ji} & \text{for } 1 \le i < j \le n. \end{cases}$$

$P^+ = P^+(2n,q)$ is the maximal parabolic subgroup of $O^+(2n,q)$ defined by:

$$P^+(2n,q) = \left\{ \left[\begin{smallmatrix} A & 0 \\ 0 & {}^tA^{-1} \end{smallmatrix}\right] \left[\begin{smallmatrix} 1_n & B \\ 0 & 1_n \end{smallmatrix}\right] \middle| A \in GL(n,q),\ \ B \ \text{ alternating} \right\}.$$

Then, with respect to $P^+ = P^+(2n,q)$, the Bruhat decomposition of $O^+(2n, q)$ is given by:

$$O^+(2n,q) = \coprod_{r=0}^{n} P^+ \sigma_r^+ P^+, \tag{17}$$

where

$$\sigma_r^+ = \begin{bmatrix} 0 & 0 & 1_r & 0 \\ 0 & 1_{n-r} & 0 & 0 \\ 1_r & 0 & 0 & 0 \\ 0 & 0 & 0 & 1_{n-r} \end{bmatrix} \in O^+(2n,q).$$

Put, for $0 \le r \le n$,

$$A_r^+ = \{w \in P^+(2n,q) \,|\, \sigma_r^+ w (\sigma_r^+)^{-1} \in P^+(2n,q)\}.$$

Expressing $O^+(2n,q)$ as a disjoint union of right cosets of $P^+ = P^+(2n,q)$, the Bruhat decomposition in (17) can be written as

$$O^+(2n,q) = \coprod_{r=0}^{n} P^+ \sigma_r^+ (A_r^+ \backslash P^+). \tag{18}$$

The order of the general linear group $GL(n,q)$ is given by

$$g_n = \prod_{j=0}^{n-1}(q^n - q^j) = q^{\binom{n}{2}} \prod_{j=1}^{n}(q^j - 1).$$

For integers n, r with $0 \le r \le n$, the q-binomial coefficients are defined as:

$$\left[\begin{smallmatrix} n \\ r \end{smallmatrix}\right]_q = \prod_{j=0}^{r-1}(q^{n-j} - 1)/(q^{r-j} - 1).$$

Then, for integers n, r with $0 \le r \le n$, we have

$$\frac{g_n}{g_{n-r}g_r} = q^{r(n-r)} \left[\begin{smallmatrix} n \\ r \end{smallmatrix}\right]_q . \tag{19}$$

As it is shown in [12],

$$|A_r^+| = g_r g_{n-r} q^{\binom{n}{2}} q^{r(2n-3r+1)/2}. \tag{20}$$

Also, it is immediate to see that

$$|P^+(2n,q)| = q^{\binom{n}{2}} g_n. \tag{21}$$

Thus we get, from (19)-(21),

$$| A_r^+ \backslash P^+(2n,q) |= \left[\begin{smallmatrix} n \\ r \end{smallmatrix}\right]_q q^{\binom{r}{2}}, \tag{22}$$

and

$$| P^+(2n,q)\sigma_r^+ P^+(2n,q) |=| P^+(2n,q) |^2| A_r^+ |^{-1}= q^{\binom{n}{2}} g_n \left[\begin{smallmatrix} n \\ r \end{smallmatrix}\right]_q q^{\binom{r}{2}}. \tag{23}$$

Let

$$DC_1^+(n,q) = P^+(2n,q)\sigma_{n-1}^+ P^+(2n,q) \text{ for } n = 2,4,6,\ldots, \tag{24}$$

$$DC_2^+(n,q) = P^+(2n,q)\sigma_{n-2}^+ P^+(2n,q) \text{ for } n = 2,4,6,\ldots, \tag{25}$$

$$DC_1^-(n,q) = P^+(2n,q)\sigma_{n-1}^+ P^+(2n,q) \text{ for } n = 1,3,5,\ldots, \tag{26}$$

$$DC_2^-(n,q) = P^+(2n,q)\sigma_{n-2}^+ P^+(2n,q) \text{ for } n = 3,5,7,\ldots. \tag{27}$$

Then, from (23), we have

$$N_i^{\pm}(n,q) = |DC_i^{\pm}(n,q)| = A_i^{\pm}(n,q)B_i^{\pm}(n,q) \text{ for } i = 1,2 \tag{28}$$

(cf. (1)-(8)).

Unless otherwise stated, from now on, we will agree that anything related to $DC_1^+(n,q)$ and $DC_1^-(n,q)$ are defined for $n = 2,4,6,\ldots$, anything related to $DC_1^-(n,q)$ for $n = 1,3,5,\ldots$, and that anything related to $DC_2^-(n,q)$ is defined for $n = 3,5,7\ldots.$

Also, from (18), (23), we have

$$|O^+(2n,q)| = \sum_{r=0}^{n} |P^+(2n,q)|^2 |A_r^+|^{-1}$$

$$= 2q^{n^2-n}(q^n-1)\prod_{j=1}^{n-1}(q^{2j}-1),$$

where one can apply the following q-binomial theorem with $x=-1$.

$$\sum_{r=0}^{n} \left[\begin{smallmatrix} n \\ r \end{smallmatrix}\right]_q (-1)^r q^{\binom{r}{2}} x^r = (x;q)_n,$$

with $(x;q)_n = (1-x)(1-qx)\cdots(1-q^{n-1}x)$ (x an indeterminate, $n \in \mathbb{Z}_{>0}$).

3. Exponential sums over double cosets of $O^+(2n, 2^r)$

The following notations will be used throughout this paper.

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

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

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

For any nontrivial additive character ψ of $\mathbb{F}_q$ and $a \in \mathbb{F}_q^*$, the Kloosterman sum $K_{GL(t,q)}(\psi; a)$ for $GL(t,q)$ is defined as

$$K_{GL(t,q)}(\psi; a) = \sum_{w \in GL(t,q)} \psi(Trw + a\ Trw^{-1}).$$

Notice that, for $t=1$, $K_{GL(1,q)}(\psi; a)$ denotes the Kloosterman sum $K(\psi; a)$.

For the Kloosterman sum $K(\psi; a)$, we have the Weil bound (cf. [15])

$$\mid K(\psi; a) \mid \leq 2\sqrt{q}. \tag{29}$$

In [8], it is shown that $K_{GL(t,q)}(\psi; a)$ satisfies the following recursive relation: for integers $t \geq 2$, $a \in \mathbb{F}_q^*$,

$$\begin{aligned} K_{GL(t,q)}(\psi; a) = {} & q^{t-1}K_{GL(t-1,q)}(\psi; a)K(\psi; a) \\ & + q^{2t-2}(q^{t-1}-1)K_{GL(t-2,q)}(\psi; a), \end{aligned} \tag{30}$$

where we understand that $K_{GL(0,q)}(\psi; a) = 1$. From (30), an explicit expression of the Kloosterman sum for $GL(t,q)$ was derived in [8].

In Section 6 of [12], it is shown that the Gauss sum for $O^+(2n,q)$ is given by:

$$\begin{aligned} \sum_{w \in O^+(2n,q)} \psi(Trw) &= \sum_{r=0}^{n} \sum_{w \in p^+ \sigma_r^+ P^+} \psi(Trw) \\ &= \sum_{r=0}^{n} |A_r^+ \backslash P^+| \sum_{w \in P^+} \psi(Trw\sigma_r^+) \\ &= q^{\binom{n}{2}} \sum_{r=0}^{n} |A_r^+ \backslash P^+| q^{r(n-r)} s_r K_{GL(n-r,q)}(\psi; 1). \end{aligned} \tag{31}$$

Here ψ is any nontrivial additive character of $\mathbb{F}_q$, $s_0 = 1$, and, for $r \in \mathbb{Z}_{>0}$, s_r denotes the number of all $r \times r$ nonsingular symmetric matrices over $\mathbb{F}_q$, which is given by

$$s_r = \begin{cases} q^{r(r+2)/4} \prod_{j=1}^{r/2} (q^{2j-1} - 1), & \text{if } r \text{ is even,} \\ q^{(r^2-1)/4} \prod_{j=1}^{(r+1)/2} (q^{2j-1} - 1), & \text{if } r \text{ is odd,} \end{cases} \tag{32}$$

(cf. [12], Proposition 4.3).

Thus we see from (31), (32), and (22) that, for each r with $0 \le r \le n$,

(33)

$$\sum_{w \in P^+ \sigma_r^+ P^+} \psi(Trw)$$
$$= \begin{cases} q^{\binom{n}{2}} q^{rn - \frac{1}{4}r^2} \left[\begin{smallmatrix} n \\ r \end{smallmatrix}\right]_q \prod_{j=1}^{r/2} (q^{2j-1} - 1) K_{GL(n-r,q)}(\psi; 1), & \text{if } r \text{ is even,} \\ q^{\binom{n}{2}} q^{rn - \frac{1}{4}(r+1)^2} \left[\begin{smallmatrix} n \\ r \end{smallmatrix}\right]_q \prod_{j=1}^{(r+1)/2} (q^{2j-1} - 1) K_{GL(n-r,q)}(\psi; 1), & \text{if } r \text{ is odd.} \end{cases}$$

For our purposes, we need four infinite families of exponential sums in (33) over $DC_1^+(n,q)$ and $DC_2^+(n,q)$ for $n = 2, 4, 6, \ldots$, $DC_1^-(n,q)$ for $n = 1, 3, 5, \ldots$, and $DC_2^-(n,q)$ for $n = 3, 5, 7, \ldots$. So we state them separately as a theorem.

Theorem 3.1. *Let ψ be any nontrivial additive character of $\mathbb{F}_q$. Then, in the notations of* (1), (3), (5), (7), *we have*

$$\sum_{w \in DC_1^{\pm}(n,q)} \psi(Trw) = A_1^{\pm}(n,q) K(\psi; 1),$$

$$\begin{aligned} \sum_{w \in DC_2^{\pm}(n,q)} \psi(Trw) &= q^{-1} A_2^{\pm}(n,q) K_{GL(2,q)}(\psi; 1) \\ &= A_2^{\pm}(n,q)(K(\psi; 1)^2 + q^2 - q) \end{aligned}$$

(*cf.* (33), (30)).

Proposition 3.2 ([11]). *For $n = 2^s (s \in \mathbb{Z}_{\ge 0})$, and ψ a nontrivial additive character of $\mathbb{F}_q$,*

$$K(\psi; a^n) = K(\psi; a).$$

We need a result of Carlitz for the next corollary.

Theorem 3.3 ([2]). *For the canonical additive character λ of $\mathbb{F}_q$, and $a \in \mathbb{F}_q^*$,*

$$K_2(\lambda; a) = K(\lambda; a)^2 - q. \tag{34}$$

The next corollary follows from Theorem 3, Proposition 4, (34), and simple change of variables.

Corollary 3.4. *Let λ be the canonical additive character of $\mathbb{F}_q$, and let $a \in \mathbb{F}_q^*$. Then we have*

$$\sum_{w \in DC_1^{\pm}(n,q)} \lambda(aTrw) = A_1^{\pm}(n,q) K(\lambda; a), \tag{35}$$

$$\begin{aligned}\sum_{w\in DC_2^{\pm}(n,q)}\lambda(aTrw)&=A_2^{\pm}(n,q)(K(\lambda;a)^2+q^2-q)\\&=A_2^{\pm}(n,q)(K_2(\lambda;a)+q^2)\end{aligned}\tag{36}$$

(*cf.* (1), (3), (5), (7)).

Proposition 3.5 ([11])**.** *Let λ be the canonical additive character of $\mathbb{F}_q$, $m\in\mathbb{Z}_{>0}$, $\beta\in\mathbb{F}_q$. Then*

$$\sum_{a\in\mathbb{F}_q^*}\lambda(-a\beta)K_m(\lambda;a)=\begin{cases}qK_{m-1}(\lambda;\beta^{-1})+(-1)^{m+1}, & \text{if } \beta\neq 0,\\ (-1)^{m+1}, & \text{if } \beta=0,\end{cases}\tag{37}$$

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

For any integer r with $0\leq r\leq n$, and each $\beta\in\mathbb{F}_q$, we let

$$N_{P^+\sigma_r^+P^+}(\beta)=|\{w\in P^+\sigma_r^+P^+\,|\,Trw=\beta\}|.$$

Then it is easy to see that

$$qN_{P^+\sigma_r^+P^+}(\beta)=|P^+\sigma_r^+P^+|+\sum_{a\in\mathbb{F}_q^*}\lambda(-a\beta)\sum_{w\in P^+\sigma_r^+P^+}\lambda(aTrw).\tag{38}$$

Now, from (35)-(38), (24)-(28), and (1)-(8), we have the following result.

Proposition 3.6.

(a)

$$\begin{aligned}&N_{DC_1^{\pm}(n,q)}(\beta)\\&=q^{-1}A_1^{\pm}(n,q)B_1^{\pm}(n,q)+q^{-1}A_1^{\pm}(n,q)\times\begin{cases}1, & \beta=0,\\ q+1, & tr(\beta^{-1})=0,\\ -q+1, & tr(\beta^{-1})=1.\end{cases}\end{aligned}\tag{39}$$

(b)

$$\begin{aligned}&N_{DC_2^{\pm}(n,q)}(\beta)\\&=q^{-1}A_2^{\pm}(n,q)B_2^{\pm}(n,q)+q^{-1}A_2^{\pm}(n,q)\times\begin{cases}qK(\lambda;\beta^{-1})-q^2-1, & \beta\neq 0,\\ q^3-q^2-1, & \beta=0.\end{cases}\end{aligned}\tag{40}$$

Corollary 3.7. (a) *For all even $n\geq 2$ and all q, $N_{DC_1^+(n,q)}(\beta)>0$ for all β.*

(b) *For all even $n\geq 4$ and all q, or $n=2$ and all $q\geq 4$, $N_{DC_2^+(n,q)}(\beta)>0$ for all β; for $n=2$ and all $q=2$,*

$$N_{DC_2^+(2,2)}(\beta)=\begin{cases}0, & \beta=1,\\ 12=|P^+(4,2)|, & \beta=0.\end{cases}$$

(c) *For all odd $n \geq 3$ and all q, $N_{DC_1^-(n,q)}(\beta) > 0$ for all β; for $n = 1$ and all q,*

$$N_{DC^-(1,q)}(\beta) = \begin{cases} 1, & \beta = 0, \\ 2, & tr(\beta^{-1}) = 0, \\ 0, & tr(\beta^{-1}) = 1. \end{cases} \tag{41}$$

(d) *For all odd $n \geq 3$ and all q, $N_{DC_2^-(n,q)}(\beta) > 0$ for all β.*

Proof. (a), (c), and (d) are left to the reader.

(b) Let $n = 2$. Let $\beta \neq 0$. Then, from (40), we have

$$N_{DC_2^+(2,q)}(0) = q^2\{q^2 - 2q - 1 + K(\lambda; \beta^{-1})\}, \tag{42}$$

where $q^2 - 2q - 1 + K(\lambda; \beta^{-1}) \geq q^2 - 2q - 1 - 2\sqrt{q} > 0$, for $q \geq 4$, by invoking the Weil bound in (29). Also, observe from (42) that $N_{DC_2^+(2,2)}(1) = 0$.

On the other hand, if $\beta = 0$, then, from (40), we get

$$N_{DC_2^+(2,q)}(0) = q^2(2q^2 - 2q - 1) > 0 \text{ for all } q \geq 2.$$

In addition, we note that $N_{DC_2^+(2,2)}(0) = 12$.

Assume now that $n \geq 4$. If $\beta = 0$, then, from (40), we see that $N_{DC_2^+(n,q)}(0) > 0$ for all q. Let $\beta \neq 0$. Then, again by invoking the Weil bound,

$$\begin{aligned} &N_{DC_2^+(n,q)}(\beta) \geq q^{-1}A_2^+(n,q) \\ &\times \{(q^n - 1)(q^{n-1} - 1)q^{\frac{1}{4}(n-4)^2-1} \prod_{j=1}^{(n-2)/2} (q^{2j} - 1) - (q^2 + 2q^{\frac{3}{2}} + 1)\}. \end{aligned}$$

Clearly, $\prod_{j=1}^{(n-2)/2}(q^{2j} - 1) > 1$. So we only need to show, for all $q \geq 2$,

$$f(q) = (q^n - 1)(q^{n-1} - 1)q^{\frac{1}{4}(n-4)^2-1} - (q^2 + 2q^{\frac{3}{2}} + 1) > 0.$$

But, as $n \geq 4$, $f(q) \geq q^{-1}(q^4 - 1)(q^3 - 1) - (q^2 + 2q^{\frac{3}{2}} + 1) > 0$ for all $q \geq 2$. □

4. Construction of codes

Here we will construct four infinite families of binary linear codes $C(DC_1^+(n,q))$ of length $N_1^+(n,q)$ for $n = 2, 4, 6, \ldots$ and all q, $C(DC_2^+(n,q))$ of length $N_2^+(n,q)$ for $n = 2, 4, 6, \ldots$ and all q, $C(DC_1^-(n,q))$ of length $N_1^-(n,q)$ for $n = 1, 3, 5, \ldots$ and all q, and $C(DC_2^-(n,q))$ of length $N_2^-(n,q)$ for $n = 3, 5, 7, \ldots$ and all q, respectively associated with the double cosets $DC_1^+(n,q)$, $DC_2^+(n,q)$, $DC_1^-(n,q)$, and $DC_2^-(n,q)$ (cf. (24)-(27)).

Let $g_1, g_2, \ldots, g_{N_i^\pm(n,q)}$ be fixed orderings of the elements in $DC_i^\pm(n,q)$ for $i = 1, 2$ by abuse of notations. Then we put

$$v_i^\pm(n,q) = (Trg_1, Trg_2, \ldots, Trg_{N_i^\pm(n,q)}) \in \mathbb{F}_q^{N_i^\pm(n,q)} \text{ for } i = 1, 2.$$

The binary codes $C(DC_1^+(n,q))$, $C(DC_2^+(n,q))$, $C(DC_1^-(n,q))$, and $C(DC_2^-(n,q))$ are defined as:

$$C(DC_i^{\pm}(n,q)) = \{u \in \mathbb{F}_2^{N_i^{\pm}(n,q)} \mid u \cdot v_i^{\pm}(n,q) = 0\} \text{ for } i = 1,2, \tag{43}$$

where the dot denotes respectively the usual inner product in $\mathbb{F}_q^{N_i^{\pm}(n,q)}$ for $i = 1,2$.

The following Delsarte's theorem is well-known.

Theorem 4.1 ([17])**.** *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 respective duals of the codes in (43) are given by:

(44)

$$\begin{aligned} &C(DC_i^{\pm}(n,q))^{\perp} \\ &= \{c_i^{\pm}(a) = c_i^{\pm}(a;n,q) = (tr(aTrg_1), \ldots, tr(aTrg_{N_i^{\pm}(n,q)})) \mid a \in \mathbb{F}_q\} \ (i=1,2). \end{aligned}$$

Let $\mathbb{F}_2^+, \mathbb{F}_q^+$ denote the additive groups of the fields $\mathbb{F}_2, \mathbb{F}_q$, respectively. Then we have the following exact sequence of groups:

$$0 \to \mathbb{F}_2^+ \to \mathbb{F}_q^+ \to \Theta(\mathbb{F}_q) \to 0,$$

where the first map is the inclusion and the second one is the Artin-Schreier operator in characteristic two given by $x \mapsto \Theta(x) = x^2 + x$. So

$$\Theta(\mathbb{F}_q) = \{\alpha^2 + \alpha \mid \alpha \in \mathbb{F}_q\}, \text{ and } [\mathbb{F}_q^+ : \Theta(\mathbb{F}_q)] = 2. \tag{45}$$

Theorem 4.2 ([11])**.** *Let λ be the canonical additive character of $\mathbb{F}_q$, and let $\beta \in \mathbb{F}_q^*$. Then*

(46)

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

if $x^2 + x + b (b \in \mathbb{F}_q)$ is irreducible over $\mathbb{F}_q$, or equivalently if $b \in \mathbb{F}_q \setminus \Theta(\mathbb{F}_q)$ (cf. (45)*).*

Theorem 4.3. (a) *The map $\mathbb{F}_q \to C(DC_1^+(n,q))^{\perp} (a \mapsto c_1^+(a))$ is an $\mathbb{F}_2$-linear isomorphism for $n \geq 2$ even and all q.*

(b) *The map $\mathbb{F}_q \to C(DC_2^+(n,q))^{\perp} (a \mapsto c_2^+(a))$ is an $\mathbb{F}_2$-linear isomorphism for $n \geq 4$ even and all q, or $n = 2$ and $q \geq 4$.*

(c) *The map $\mathbb{F}_q \to C(DC_1^-(n,q))^{\perp} (a \mapsto c_1^-(a))$ is an $\mathbb{F}_2$-linear isomorphism for $n \geq 3$ odd and all q, or $n = 1$ and $q \geq 8$.*

(d) *The map $\mathbb{F}_q \to C(DC_2^-(n,q))^{\perp} (a \mapsto c_2^-(a))$ is an $\mathbb{F}_2$-linear isomorphism for $n \geq 3$ odd and all q.*

Proof. All maps are clearly $\mathbb{F}_2$-linear and surjective. Let a be in the kernel of map $\mathbb{F}_q \to C(DC_1^+(n,q))^\perp$ $(a \mapsto c_1^+(a))$. Then $tr(aTrg) = 0$ for all $g \in DC_1^+(n,q)$. Since, by Corollary 9(a), $Tr : DC_1^+(n,q) \to \mathbb{F}_q$ is surjective, $tr(a\alpha) = 0$ for all $\alpha \in \mathbb{F}_q$. This implies that $a = 0$, since otherwise $tr : \mathbb{F}_q \to \mathbb{F}_2$ would be the zero map. This shows (a). All the other assertions can be handled in the same way, except for $n = 1$ and $q \geq 8$ case of (c). Assume that we are in that case. Then, by (41), $tr(a\beta) = 0$ for all $\beta \in \mathbb{F}_q^*$ with $tr(\beta^{-1}) = 0$. Hilbert's theorem 90 says that $tr(\gamma) = 0 \Leftrightarrow \gamma = \alpha^2 + \alpha$ for some $\alpha \in \mathbb{F}_q$, and hence $\sum_{\alpha \in \mathbb{F}_q - \{0,1\}} \lambda(\frac{a}{\alpha^2+\alpha}) = q - 2$. If $a \neq 0$, then, using (46) and the Weil bound (29), we would have

$$q - 2 = \sum_{\alpha \in \mathbb{F}_q - \{0,1\}} \lambda(\frac{a}{\alpha^2 + \alpha}) = K(\lambda; a) - 1 \leq 2\sqrt{q} - 1.$$

But this is impossible, since $x > 2\sqrt{x} + 1$ for $x \geq 8$. □

Remark. One can show that the kernel of the map

$$\mathbb{F}_q \to C(DC_2^+(2,2))^\perp (a \mapsto c_2^+(a)),$$

and the maps $\mathbb{F}_q \to C(DC_1^-(1,q))^\perp (a \mapsto c_1^-(a))$, for $q = 2, 4$, are all equal to $\mathbb{F}_2$.

5. Recursive formulas for power moments of Kloosterman sums

Here we will be able to find, via Pless' power moment identity, infinite families of recursive formulas generating power moments of Kloosterman and 2-dimensional Kloosterman sums over all $\mathbb{F}_q$ (with three exceptions) in terms of the frequencies of weights in $C(DC_1^+(n,q))$ or $C(DC_1^-(n,q))$, and $C(DC_2^+(n,q))$ or $C(DC_2^-(n,q))$, respectively.

Theorem 5.1 (Pless' power moment identity, [17])**.** *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 $h = 0, 1, 2, \ldots,$*

$$(47) \qquad \sum_{j=0}^{n} j^h B_j = \sum_{j=0}^{\min\{n,h\}} (-1)^j B_j^\perp \sum_{t=j}^{h} t! S(h,t) q^{k-t} (q-1)^{t-j} \binom{n-j}{n-t},$$

where $S(h,t)$ is the Stirling number of the second kind defined in (11)*.*

Lemma 5.2. *Let*

$$c_i^\pm(a) = (tr(aTrg_1), \ldots, tr(aTrg_{N_i^\pm(n,q)})) \in C(DC_i^\pm(n,q))^\perp$$

for $i = 1, 2$, and $a \in \mathbb{F}_q^*$. Then the Hamming weights $w(c_1^\pm(a))$ and $w(c_2^\pm(a))$ are expressed as follows:

$$(48) \qquad \text{(a)} \;\; w(c_1^\pm(a)) = \frac{1}{2} A_1^\pm(n,q)(B_1^\pm(n,q) - K(\lambda; a)),$$

$$\text{(49)} \qquad \text{(b)}\ w(c_2^{\pm}(a)) = \frac{1}{2}A_2^{\pm}(n,q)(B_2^{\pm}(n,q) - q^2 + q - K(\lambda;a)^2)$$

$$\text{(50)} \qquad = \frac{1}{2}A_2^{\pm}(n,q)(B_2^{\pm}(n,q) - q^2 - K_2(\lambda;a))$$

(*cf.* (1)-(8)).

Proof.

$$w(c_i^{\pm}(a)) = \frac{1}{2}\sum_{j=1}^{N_i^{\pm}(n,q)}(1-(-1)^{tr(aTrg_j)}) = \frac{1}{2}(N_i^{\pm}(n,q) - \sum_{w\in DC_i^{\pm}(n,q)}\lambda(aTrw))$$

for $i = 1, 2$. Our results now follow from (28) and (34)-(36). □

Let $u = (u_1, \ldots, u_{N_i^{\pm}(n,q)}) \in \mathbb{F}_2^{N_i^{\pm}(n,q)}$ for $i = 1, 2$, with ν_β 1's in the coordinate places where $Tr(g_j) = \beta$ for each $\beta \in \mathbb{F}_q$. Then from the definition of the codes $C(DC_i^{\pm}(n,q))$ (cf. (43)) 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 $\prod_{\beta\in\mathbb{F}_q}\binom{N_{DC_i^{\pm}(n,q)}(\beta)}{\nu_\beta}$ many such codewords with weight j, we obtain the following result.

Proposition 5.3. *Let* $\{C_{i,j}^{\pm}(n,q)\}_{j=0}^{N_i^{\pm}(n,q)}$ *be the weight distribution of*

$$C(DC_i^{\pm}(n,q))$$

for $i = 1, 2$. *Then we have*

$$\text{(51)} \qquad C_{i,j}^{\pm}(n,q) = \sum\prod_{\beta\in\mathbb{F}_q}\binom{N_{DC_i^{\pm}(n,q)}(\beta)}{\nu_\beta} \ \text{for}\ 0 \le j \le N_i^{\pm}(n,q)\ \text{and}\ i = 1, 2,$$

where the sum is over all the sets of integers $\{\nu_\beta\}_{\beta\in\mathbb{F}_q}(0 \le \nu_\beta \le N_{DC_i^{\pm}(n,q)}(\beta))$, *satisfying*

$$\text{(52)} \qquad \sum_{\beta\in\mathbb{F}_q}\nu_\beta = j \ \text{and}\ \sum_{\beta\in\mathbb{F}_q}\nu_\beta\beta = 0.$$

Corollary 5.4. *Let* $\{C_{i,j}^{\pm}(n,q)\}_{j=0}^{N_i^{\pm}(n,q)}$ *be the weight distribution of*

$$C(DC_i^{\pm}(n,q))$$

for $i = 1, 2$. *Then we have*

$$C_{i,j}^{\pm}(n,q) = C_{i,N_i^{\pm}(n,q)-j}^{\pm}(n,q) \ \text{for all}\ j, \ \text{with}\ 0 \le j \le N_i^{\pm}(n,q).$$

Proof. Under the replacements $\nu_\beta \to N_{DC_i^{\pm}(n,q)}(\beta) - \nu_\beta$ for each $\beta \in \mathbb{F}_q$, the first equation in (52) is changed to $N_i^{\pm}(n,q) - j$, while the second one in there and the summands in (51) are left unchanged. The second sum in (52) is left unchanged, since $\sum_{\beta\in\mathbb{F}_q} N_{DC_i^{\pm}(n,q)}(\beta)\beta = 0$, as one can see by using the explicit expressions of $N_{DC^{\mp}(n,q)}(\beta)$ in (39) and (40). □

Theorem 5.5 ([14]). *Let $q = 2^r$, with $r \geq 2$. Then the range R of $K(\lambda; a)$, as a varies over $\mathbb{F}_q^*$, is given by:*

$$R = \{\tau \in \mathbb{Z} \mid |\tau| < 2\sqrt{q},\ \tau \equiv -1 \pmod 4\}.$$

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

The formulas appearing in the next theorem and stated in (10) and (14) follow by applying the formula in (51) to each $C(DC_i^{\pm}(n,q))$, using the explicit values of $N_{DC_i^{\pm}(n,q)}(\beta)$ in (39) and (40), and taking Theorem 5.5 into consideration.

Theorem 5.6. *Let $\{C_{i,j}^{\pm}(n,q)\}_{j=0}^{N_i^{\pm}(n,q)}$ be the weight distribution of*

$$C(DC_i^{\pm}(n,q))$$

for $i = 1, 2$, and assume that $q \geq 4$ for $C(DC_2^{\pm}(n,q))$. Then we have

(a) *For $j = 0, \ldots, N_1^{\pm}(n,q)$,*

$$\begin{aligned} C_{1,j}^{\pm}(n,q) = & \sum \binom{q^{-1}A_1^{\pm}(n,q)(B_1^{\pm}(n,q)+1)}{\nu_0} \\ & \times \prod_{tr(\beta^{-1})=0} \binom{q^{-1}A_1^{\pm}(n,q)(B_1^{\pm}(n,q)+q+1)}{\nu_\beta} \\ & \times \prod_{tr(\beta^{-1})=1} \binom{q^{-1}A_1^{\pm}(n,q)(B_1^{\pm}(n,q)-q+1)}{\nu_\beta}, \end{aligned}$$

where the sum is over all the sets of nonnegative integers $\{\nu_\beta\}_{\beta\in\mathbb{F}_q}$ satisfying $\sum_{\beta\in\mathbb{F}_q} \nu_\beta = j$ and $\sum_{\beta\in\mathbb{F}_q} \nu_\beta\beta = 0$.

(b) *For $j = 0, \ldots, N_2^{\pm}(n,q)$,*

$$\begin{aligned} C_{2,j}^{\pm}(n,q) = & \sum \binom{q^{-1}A_2^{\pm}(n,q)(B_2^{\pm}(n,q)+q^3-q^2-1)}{\nu_0} \\ & \times \prod_{\substack{|\tau|<2\sqrt{q} \\ \tau\equiv -1(4)}} \prod_{K(\lambda;\beta^{-1})=\tau} \binom{q^{-1}A_2^{\pm}(n,q)(B_2^{\pm}(n,q)+q\tau-q^2-1)}{\nu_\beta}, \end{aligned}$$

where the sum is over all the sets of nonnegative integers $\{\nu_\beta\}_{\beta\in\mathbb{F}_q}$ satisfying $\sum_{\beta\in\mathbb{F}_q} \nu_\beta = j$, and $\sum_{\beta\in\mathbb{F}_q} \nu_\beta\beta = 0$.

From now on, we will assume that, for $C(DC_1^{+}(n,q))^{\perp}$, $n \geq 2$ even and all q; for $C(DC_2^{+}(n,q))^{\perp}$, $n \geq 2$ even and $q \geq 4$; for $C(DC_1^{-}(n,q))^{\perp}$, either $n \geq 3$ odd and all q, or $n = 1$ and $q \geq 8$; for $C(DC_2^{-}(n,q))^{\perp}$, $n \geq 3$ odd and $q \geq 4$.

Under these assumptions, each codeword in $C(DC_i^{\pm}(n,q))^{\perp}$ can be written as $c_i^{\pm}(a)$ for $i = 1, 2$, and a unique $a \in \mathbb{F}_q$ (cf. Theorem 12, (44)).

Now, we apply the Pless' power moment identity in (47) to $C(DC_i^{\pm}(n,q))^{\perp}$, for those values of n and q, in order to get the results in Theorem 1.1 (cf. (9), (12), (13)) about recursive formulas.

The left hand side of that identity in (47) is equal to

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

with $w(c_i^{\pm}(a))$ given by (48)-(50). We have

$$\begin{aligned}\sum_{a \in \mathbb{F}_q^*} w(c_1^{\pm}(a))^h &= \frac{1}{2^h} A_1^{\pm}(n,q)^h \sum_{a \in \mathbb{F}_q^*} (B_1^{\pm}(n,q) - K(\lambda; a))^h \\ &= \frac{1}{2^h} A_1^{\pm}(n,q)^h \sum_{l=0}^{h} (-1)^l \binom{h}{l} B_1^{\pm}(n,q)^{h-l} MK^l. \qquad (53)\end{aligned}$$

Similarly, we have

(54)

$$\begin{aligned}\sum_{a \in \mathbb{F}_q^*} w(c_2^{\pm}(a))^h &= \frac{1}{2^h} A_2^{\pm}(n,q)^h \sum_{l=0}^{h} (-1)^l \binom{h}{l} (B_2^{\pm}(n,q) - q^2 + q)^{h-l} MK^{2l} \\ &= \frac{1}{2^h} A_2^{\pm}(n,q)^h \sum_{l=0}^{h} (-1)^l \binom{h}{l} (B_2^{\pm}(n,q) - q^2)^{h-l} MK_2^l. \qquad (55)\end{aligned}$$

Note here that, in view of (34), obtaining power moments of 2-dimensional Kloosterman sums is equivalent to getting even power moments of Kloosterman sums. Also, one has to separate the term corresponding to $l = h$ in (53)-(55), and notes $\dim_{\mathbb{F}_2} C(DC_i^{\pm}(n,q))^{\perp} = r$.

References

[1] L. Carlitz, *Gauss sums over finite fields of order* 2^n, Acta Arith. **15** (1968/1969), 247–265. https://doi.org/10.4064/aa-15-3-247-265

[2] ———, *A note on exponential sums*, Pacific J. Math. **30** (1969), 35–37. http://projecteuclid.org/euclid.pjm/1102978697

[3] P. Charpin, T. Helleseth, and V. Zinoviev, *Propagation characteristics of $x \mapsto x^{-1}$ and Kloosterman sums*, Finite Fields Appl. **13** (2007), no. 2, 366–381. https://doi.org/10.1016/j.ffa.2005.08.007

[4] J.-M. Deshouillers and H. Iwaniec, *Kloosterman sums and Fourier coefficients of cusp forms*, Invent. Math. **70** (1982/83), no. 2, 219–288. https://doi.org/10.1007/BF01390728

[5] H. Dobbertin, P. Felke, T. Helleseth, and P. Rosendahl, *Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums*, IEEE Trans. Inform. Theory **52** (2006), no. 2, 613–627. https://doi.org/10.1109/TIT.2005.862094

[6] R. Evans, *Seventh power moments of Kloosterman sums*, Israel J. Math. **175** (2010), 349–362. https://doi.org/10.1007/s11856-010-0014-0

[7] 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), no. 3, 263–289. https://doi.org/10.1515/advg.2001.017

[8] D. S. Kim, *Gauss sums for symplectic groups over a finite field*, Monatsh. Math. **126** (1998), no. 1, 55–71. https://doi.org/10.1007/BF01312455

[9] ———, *Infinite families of recursive formulas generating power moments of ternary Kloosterman sums with square arguments arising from symplectic groups*, Adv. Math. Commun. **3** (2009), no. 2, 167–178. https://doi.org/10.3934/amc.2009.3.167

[10] ———, *Codes associated with special linear groups and power moments of multi-dimensional Kloosterman sums*, Ann. Mat. Pura Appl. (4) **190** (2011), no. 1, 61–76. https://doi.org/10.1007/s10231-010-0138-1

[11] ———, *Codes associated with $O^+(2n, 2^r)$ and power moments of Kloosterman sums*, Integers **12** (2012), no. 2, 237–257. https://doi.org/10.1515/integ.2011.100

[12] D. S. Kim and Y. H. Park, *Gauss sums for orthogonal groups over a finite field of characteristic two*, Acta Arith. **82** (1997), no. 4, 331–357. https://doi.org/10.4064/aa-82-4-331-357

[13] H. D. Kloosterman, *On the representation of numbers in the form $ax^2+by^2+cz^2+dt^2$*, Acta Math. **49** (1927), no. 3-4, 407–464. https://doi.org/10.1007/BF02564120

[14] G. Lachaud and J. Wolfmann, *The weights of the orthogonals of the extended quadratic binary Goppa codes*, IEEE Trans. Inform. Theory **36** (1990), no. 3, 686–692. https://doi.org/10.1109/18.54892

[15] R. Lidl and H. Niederreiter, *Finite Fields*, second edition, Encyclopedia of Mathematics and its Applications, **20**, Cambridge University Press, Cambridge, 1997.

[16] R. Livné, *Motivic orthogonal two-dimensional representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Israel J. Math. **92** (1995), no. 1-3, 149–156. https://doi.org/10.1007/BF02762074

[17] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes. II*, North-Holland Publishing Co., Amsterdam, 1977.

[18] M. J. Moisio, *The moments of a Kloosterman sum and the weight distribution of a Zetterberg-type binary cyclic code*, IEEE Trans. Inform. Theory **53** (2007), no. 2, 843–847. https://doi.org/10.1109/TIT.2006.889020

[19] 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.

[20] H. Salié, *Über die Kloostermanschen Summen $S(u, v; q)$*, Math. Z. **34** (1931), 91–109.

[21] R. Schoof and M. van der Vlugt, *Hecke operators and the weight distributions of certain codes*, J. Combin. Theory Ser. A **57** (1991), no. 2, 163–186. https://doi.org/10.1016/0097-3165(91)90016-A

Dae San Kim
Department of Mathematics
Sogang University
Seoul 04107, Korea
Email address: dskim@sogang.ac.kr