

RECURSIVE FORMULAS GENERATING POWER MOMENTS OF TERNARY KLOOSTERMAN SUMS WITH TRACE NONZERO SQUARE ARGUMENTS: $O(2n + 1, 3^r)$ CASE

DAE SAN KIM*

ABSTRACT. In this paper, we construct four infinite families of ternary linear codes associated with double cosets in $O(2n + 1, q)$ with respect to certain maximal parabolic subgroup of the special orthogonal group $SO(2n + 1, q)$. Here q is a power of three. Then we obtain two infinite families of recursive formulas, the one generating the power moments of Kloosterman sums with “trace nonzero square arguments” and the other generating the even power moments of those. Both of these families are expressed in terms of the frequencies of weights in the codes associated with those double cosets in $O(2n + 1, q)$ and in the codes associated with similar double cosets in the symplectic group $Sp(2n, q)$. 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 group $O(2n + 1, q)$.

Keywords: power moment, Kloosterman sum, trace nonzero square argument, orthogonal group, symplectic group, double cosets, maximal parabolic subgroup, Pless power moment identity, weight distribution, Gauss sum.

MSC(2010): Primary: 11T23; Secondary: 20G40, 94B05.

1. Introduction

Let ψ be a nontrivial additive character of the finite field \mathbb{F}_q with $q = p^r$ elements (p a prime). Then the Kloosterman sum $K(\psi; a)$ ([14]) is defined as

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

The Kloosterman sum was introduced in 1926 ([13]) to give an estimate for the Fourier coefficients of modular forms.

Date: Received: 4 July 2019, Accepted: 4 December 2019.

*Corresponding author.

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 .

For brief history of explicit computations on power moments of Kloosterman sums, we let the reader refer to the papers [1, 3, 14, 19, 20] and Introduction of the recent paper [11]. Exponential sums in general and Kloosterman sums in particular have found numerous applications in communication theory. For these, one may refer to the two survey papers [4] and [18]. Incomplete Kloosterman sums are also important for such applications. For example, in a recent paper [12] it is shown that the cross-correlation of the family of the sequences can be expressed in terms of the incomplete Kloosterman sum summed over the nonzero squares in the finite field. Likewise, with the well-known connection between the power moments of Kloosterman sums and Kloosterman sum itself in mind, we hope that the incomplete power moments of Kloosterman sums will also find their applications in communication theory.

From now on, let us assume that $q = 3^r$. Recently, Moisiso was able to find explicit expressions of MK^h , for $h \leq 10$ (cf. [17]). This was done, via Pless power moment identity, by connecting moments of Kloosterman sums and the frequencies of weights in the ternary Melas code of length $q - 1$, which were known by the work of Geer, Schoof and Vlught in [2].

In order to describe our results, we introduce three incomplete power moments of Kloosterman sums. For every nonnegative integer h , and ψ as before, we define

$$(1.1) \quad T_0SK(\psi)^h = \sum_{a \in \mathbb{F}_q^*, tra=0} K(\psi; a^2)^h, \quad T_{12}SK(\psi)^h = \sum_{a \in \mathbb{F}_q^*, tra \neq 0} K(\psi; a^2)^h,$$

which will be respectively called the h -th moment of Kloosterman sums with “trace zero square arguments” and those with “trace nonzero square arguments.” Then, clearly we have

$$(1.2) \quad 2SK(\psi)^h = T_0SK(\psi)^h + T_{12}SK(\psi)^h,$$

where

$$(1.3) \quad SK(\psi)^h = \sum_{a \in \mathbb{F}_q^*, a \text{ square}} K(\psi; a)^h,$$

called the h -th moment of Kloosterman sums with “square arguments.” If $\psi = \lambda$ is the canonical additive character of \mathbb{F}_q , then $SK(\lambda)^h$, $T_0SK(\lambda)^h$, and $T_{12}SK(\lambda)^h$ will be respectively denoted by SK^h , T_0SK^h , and $T_{12}SK^h$, for brevity.

In this paper, we will obtain two infinite families of recursive formulas, the one generating the power moments of Kloosterman sums with trace nonzero square arguments and the other generating the even power moments of those. To do that, we construct four infinite families of ternary linear codes associated with double cosets in $O(2n + 1, q)$ with respect to certain maximal parabolic subgroup of the special orthogonal group $SO(2n + 1, q)$, and express those power moments in terms of the frequencies of weights in the codes(cf.[9]). 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 group $O(2n + 1, q)$ [7], we can express the weight of each codeword in the duals of the codes in terms of Kloosterman sums. Then our formulas will follow immediately from the Pless power moment identity.

There have been such results as [17] and [20], as to the explicit evaluations of the power moments of Kloosterman sums. However, there have been none until the paper [8] appeared, as to the incomplete power moments of Kloosterman sums. The present paper is also about such incomplete moments. In addition, we are able to obtain not a few recursive formulas but infinite families of those producing such incomplete power moments of Kloosterman sums. Admittedly, our results are not so simple but give nice connections among number theory, coding theory and finite classical groups. Note here that in the present paper we get an infinite family of the power moments of Kloosterman sums with trace nonzero square arguments, while in [8] we obtained that with nonzero square arguments. So the two incomplete power moments are summed over the different subsets of arguments in the multiplicative group of the finite field. The approach of this paper is analogous to that of [8], but the adoption of symplectic and orthogonal groups produces the results about different incomplete moments of Kloosterman sums.

The following Theorem 1.1 is the main result of this paper. Henceforth, we agree that, for nonnegative integers a, b, c ,

$$(1.4) \quad \binom{c}{a, b} = \frac{c!}{a!b!(c-a-b)!}, \text{ if } a + b \leq c,$$

$$(1.5) \quad \binom{c}{a, b} = 0, \text{ if } a + b > c.$$

To simplify notations, we introduce the following ones which will be used throughout this paper at various places.

$$(1.6) \quad A^-(n, q) = q^{\frac{1}{4}(5n^2-1)} \begin{bmatrix} n \\ 1 \end{bmatrix}_q \prod_{j=1}^{(n-1)/2} (q^{2j-1} - 1),$$

$$(1.7) \quad B^-(n, q) = q^{\frac{1}{4}(n-1)^2} (q^n - 1) \prod_{j=1}^{(n-1)/2} (q^{2j} - 1),$$

$$(1.8) \quad A^+(n, q) = q^{\frac{1}{4}(5n^2-2n)} \begin{bmatrix} n \\ 2 \end{bmatrix}_q \prod_{j=1}^{(n-2)/2} (q^{2j-1} - 1),$$

$$(1.9) \quad B^+(n, q) = q^{\frac{1}{4}(n-2)^2} (q^n - 1)(q^{n-1} - 1) \prod_{j=1}^{(n-2)/2} (q^{2j} - 1).$$

From now on, it is assumed that either + signs or - signs are chosen everywhere, whenever \pm signs appear.

Theorem 1.1. (1) For each odd integer $n \geq 1$, all q , and $h=1,2,3,\dots$,

$$(1.10) \quad \begin{aligned} & ((-1)^{h+1} + 2^{-h}) T_{12} S K^h \\ &= - \sum_{j=1}^{h-1} ((-1)^{j+1} + 2^{-j}) \binom{h}{j} B^-(n, q)^{h-j} T_{12} S K^j \\ &+ q A^-(n, q)^{-h} \sum_{j=0}^{\min\{N_i^-(n, q), h\}} (-1)^j (C_{i,j}^-(n, q) - C_j^-(n, q)) \\ &\quad \times \sum_{t=j}^h t! S(h, t) 3^{h-t} 2^{t-h-j} \binom{N_i^-(n, q) - j}{N_i^-(n, q) - t} (i = 1, 2), \end{aligned}$$

where $N_i^-(n, q) = |DC_i^-(n, q)| = A^-(n, q)B^-(n, q)$, for $i = 1, 2$, and $\{C_{1,j}^-(n, q)\}_{j=0}^{N_1^-(n, q)}$, $\{C_{2,j}^-(n, q)\}_{j=0}^{N_2^-(n, q)}$, and $\{C_j^-(n, q)\}_{j=0}^{N_i^-(n, q)}$ are respectively the weight distributions of the ternary linear codes $C(DC_1^-(n, q))$, $C(DC_2^-(n, q))$, and $C(DC^-(n, q))$ given by:

$$(1.11) \quad \begin{aligned} C_{1,j}^-(n, q) &= \sum \binom{q^{-1}A^-(n, q)(B^-(n, q) + 1)}{\nu_0, \mu_0} \binom{q^{-1}A^-(n, q)(B^-(n, q) + 1)}{\nu_2, \mu_2} \\ &\quad \times \prod_{\beta^2 - 2\beta \neq 0 \text{ square}} \binom{q^{-1}A^-(n, q)(B^-(n, q) + q + 1)}{\nu_\beta, \mu_\beta} \\ &\quad \times \prod_{\beta^2 - 2\beta \text{ nonsquare}} \binom{q^{-1}A^-(n, q)(B^-(n, q) - q + 1)}{\nu_\beta, \mu_\beta}, \end{aligned}$$

$$C_{2,j}^-(n, q) = \sum \binom{q^{-1}A^-(n, q)(B^-(n, q) + 1)}{\nu_0, \mu_0} \binom{q^{-1}A^-(n, q)(B^-(n, q) + 1)}{\nu_1, \mu_1}$$

$$(1.12) \quad \begin{aligned} & \times \prod_{\substack{\beta^2+2\beta \neq 0 \\ \text{square}}} \binom{q^{-1}A^-(n, q)(B^-(n, q) + q + 1)}{\nu_\beta, \mu_\beta} \\ & \times \prod_{\substack{\beta^2+2\beta \\ \text{nonsquare}}} \binom{q^{-1}A^-(n, q)(B^-(n, q) - q + 1)}{\nu_\beta, \mu_\beta}, \end{aligned}$$

$$(1.13) \quad \begin{aligned} C_j^-(n, q) &= \sum \binom{q^{-1}A^-(n, q)(B^-(n, q) + 1)}{\nu_1, \mu_1} \binom{q^{-1}A^-(n, q)(B^-(n, q) + 1)}{\nu_{-1}, \mu_{-1}} \\ & \times \prod_{\substack{\beta^2-1 \neq 0 \\ \text{square}}} \binom{q^{-1}A^-(n, q)(B^-(n, q) + q + 1)}{\nu_\beta, \mu_\beta} \\ & \times \prod_{\substack{\beta^2-1 \\ \text{nonsquare}}} \binom{q^{-1}A^-(n, q)(B^-(n, q) - q + 1)}{\nu_\beta, \mu_\beta} \text{ (cf. (1.4), (1.5)).} \end{aligned}$$

Here the first sum in (1.10) is 0 if $h = 1$ and the unspecified sums in (1.11), (1.12), and (1.13) run over all the sets of nonnegative integers $\{\nu_\beta\}_{\beta \in \mathbb{F}_q}$, and $\{\mu_\beta\}_{\beta \in \mathbb{F}_q}$ satisfying

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

In addition, $S(h, t)$ is the Stirling number of the second kind defined by

$$(1.14) \quad S(h, t) = \frac{1}{t!} \sum_{j=0}^t (-1)^{t-j} \binom{t}{j} j^h.$$

(2) For each even integer $n \geq 2$, all q , and $h = 1, 2, 3, \dots$,

$$(1.15) \quad \begin{aligned} & ((-1)^{h+1} + 2^{-h}) T_{12} S K^{2h} \\ &= - \sum_{j=0}^{h-1} \binom{h}{j} \{(-1)^{j+1} (B^+(n, q) - q^2 + q)^{h-j} \\ & \quad + 2^{-j} (B^+(n, q) + \frac{1}{2}q^2 - \frac{1}{2}q)^{h-j}\} T_{12} S K^{2j} \\ & \quad + q A^+(n, q)^{-h} \sum_{j=0}^{\min\{N_i^+(n, q), h\}} (-1)^j (C_{i,j}^+(n, q) - C_j^+(n, q)) \\ & \quad \times \sum_{t=j}^h t! S(h, t) 3^{h-t} 2^{t-h-j} \binom{N_i^+(n, q) - j}{N_i^+(n, q) - t} \quad (i = 1, 2), \end{aligned}$$

where $N_i^+(n, q) = |DC_i^+(n, q)| = A^+(n, q)B^+(n, q)$, for $i = 1, 2$, and $\{C_{1,j}^+(n, q)\}_{j=0}^{N_1^+(n, q)}$, $\{C_{2,j}^+(n, q)\}_{j=0}^{N_2^+(n, q)}$, and $\{C_j^+(n, q)\}_{j=0}^{N_i^+(n, q)}$ are respectively the weight distributions of the ternary linear codes $C(DC_1^+(n, q))$,

$C(DC_2^+(n, q))$, and $C(DC^+(n, q))$ given by:

$$(1.16) \quad C_{1,j}^+(n, q) = \sum \left(\begin{array}{c} q^{-1}A^+(n, q)(B^+(n, q) + q\delta(2, q; 0) + (q-1)^3) \\ \nu_1, \mu_1 \end{array} \right) \\ \times \prod_{\beta \neq 1} \left(\begin{array}{c} q^{-1}A^+(n, q)(B^+(n, q) + q\delta(2, q; \beta - 1) - 2q^2 + 3q - 1) \\ \nu_\beta, \mu_\beta \end{array} \right),$$

$$(1.17) \quad C_{2,j}^+(n, q) = \sum \left(\begin{array}{c} q^{-1}A^+(n, q)(B^+(n, q) + q\delta(2, q; 0) + (q-1)^3) \\ \nu_{-1}, \mu_{-1} \end{array} \right) \\ \times \prod_{\beta \neq -1} \left(\begin{array}{c} q^{-1}A^+(n, q)(B^+(n, q) + q\delta(2, q; \beta + 1) - 2q^2 + 3q - 1) \\ \nu_\beta, \mu_\beta \end{array} \right),$$

$$(1.18) \quad C_j^+(n, q) = \sum \left(\begin{array}{c} q^4(\delta(2, q; 0) + q^5 - q^2 - 3q + 3) \\ \nu_0, \mu_0 \end{array} \right) \\ \times \prod_{\beta \in \mathbb{F}_q^*} \left(\begin{array}{c} q^4(\delta(2, q; \beta) + q^5 - q^3 - q^2 - 2q + 3) \\ \nu_\beta, \mu_\beta \end{array} \right) \text{ (cf. (1.4), (1.5)).}$$

Here the sums are over all the sets of nonnegative integers $\{\nu_\beta\}_{\beta \in \mathbb{F}_q}$ and $\{\mu_\beta\}_{\beta \in \mathbb{F}_q}$ satisfying

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

and $\delta(2, q; \beta) = |\{(\alpha_1, \alpha_2) \in \mathbb{F}_q^2 \mid \alpha_1 + \alpha_2 + \alpha_1^{-1} + \alpha_2^{-1} = \beta\}|$.

2. $O(2n+1, q)$

For more details about this section, one is referred to the paper [7]. Throughout this paper, the following notations will be used:

$$q = 3^r \quad (r \in \mathbb{Z}_{>0}),$$

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

$\text{Tr}A$ = the trace of A for a square matrix A ,

tB = the transpose of B for any matrix B .

The orthogonal group $O(2n+1, q)$ is defined as:

$$O(2n+1, q) = \{w \in GL(2n+1, q) \mid {}^t w J w = J\},$$

where

$$J = \begin{bmatrix} 0 & 1_n & 0 \\ 1_n & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

It consists of the matrices

$$\begin{bmatrix} A & B & e \\ C & D & f \\ g & h & i \end{bmatrix} (A, B, C, D \ n \times n, e, f \ n \times 1, g, h \ 1 \times n, i \ 1 \times 1)$$

in $GL(2n+1, q)$ satisfying the relations:

$$\begin{aligned} {}^tAC + {}^tCA + {}^tgg &= 0, & {}^tBD + {}^tDB + {}^thh &= 0, \\ {}^tAD + {}^tCB + {}^tgh &= 1_n, & {}^tef + {}^tfe + i^2 &= 1, \\ {}^tAf + {}^tCe + {}^tgi &= 0, & {}^tBf + {}^tDe + {}^thi &= 0. \end{aligned}$$

Let $P(2n+1, q)$ be the maximal parabolic subgroup of $O(2n+1, q)$ given by

$$\begin{aligned} P &= P(2n+1, q) \\ &= \left\{ \begin{bmatrix} A & 0 & 0 \\ 0 & {}^tA^{-1} & 0 \\ 0 & 0 & i \end{bmatrix} \begin{bmatrix} 1_n & B & -{}^th \\ 0 & 1_n & 0 \\ 0 & h & 1 \end{bmatrix} \mid \begin{array}{l} A \in GL(n, q), \ i = \pm 1 \\ B + {}^tB + {}^thh = 0 \end{array} \right\}, \end{aligned}$$

and let $Q = Q(2n+1, q)$ be the subgroup of $P(2n+1, q)$ of index 2 defined by

$$Q = Q(2n+1, q) = \left\{ \begin{bmatrix} A & 0 & 0 \\ 0 & {}^tA^{-1} & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1_n & B & -{}^th \\ 0 & 1_n & 0 \\ 0 & h & 1 \end{bmatrix} \mid \begin{array}{l} A \in GL(n, q) \\ B + {}^tB + {}^thh = 0 \end{array} \right\}.$$

Then we see that

$$(2.1) \quad P(2n+1, q) = Q(2n+1, q) \amalg \rho Q(2n+1, q),$$

with

$$\rho = \begin{bmatrix} 1_n & 0 & 0 \\ 0 & 1_n & 0 \\ 0 & 0 & -1 \end{bmatrix}.$$

Let σ_r denote the following matrix in $O(2n+1, q)$

$$\sigma_r = \begin{bmatrix} 0 & 0 & 1_r & 0 & 0 \\ 0 & 1_{n-r} & 0 & 0 & 0 \\ 1_r & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1_{n-r} & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad (0 \leq r \leq n).$$

Then the Bruhat decomposition of $O(2n+1, q)$ with respect to $P = P(2n+1, q)$ is given by

$$(2.2) \quad \begin{aligned} O(2n+1, q) &= \prod_{r=0}^n P\sigma_r P = \prod_{r=0}^n P\sigma_r Q \\ &= \prod_{r=0}^n Q\sigma_r Q \amalg \prod_{r=0}^n \rho Q\sigma_r Q, \end{aligned}$$

which can further be modified as

$$(2.3) \quad \begin{aligned} O(2n+1, q) &= \prod_{r=0}^n P\sigma_r(B_r \setminus Q) \\ &= \prod_{r=0}^n Q\sigma_r(B_r \setminus Q) \amalg \prod_{r=0}^n \rho Q\sigma_r(B_r \setminus Q), \end{aligned}$$

with

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

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

$$\begin{bmatrix} n \\ r \end{bmatrix}_q = \prod_{j=0}^{r-1} (q^{n-j} - 1) / (q^{r-j} - 1).$$

It is shown in [7] that

$$(2.4) \quad |B_r(q) \setminus Q(2n+1, q)| = q^{\binom{r+1}{2}} \begin{bmatrix} n \\ r \end{bmatrix}_q,$$

$$(2.5) \quad \begin{aligned} |Q(2n+1, q)\sigma_r Q(2n+1, q)| &= |\rho Q(2n+1, q)\sigma_r Q(2n+1, q)| \\ &= q^{n^2} \prod_{j=1}^n (q^j - 1) q^{\binom{r}{2}} q^r \begin{bmatrix} n \\ r \end{bmatrix}_q. \end{aligned}$$

Let

$$(2.6) \quad DC_1^-(n, q) = Q(2n+1, q)\sigma_{n-1}Q(2n+1, q), \quad \text{for } n = 1, 3, 5, \dots,$$

$$(2.7) \quad DC_2^-(n, q) = \rho Q(2n+1, q)\sigma_{n-1}Q(2n+1, q), \quad \text{for } n = 1, 3, 5, \dots,$$

$$(2.8) \quad DC_1^+(n, q) = Q(2n+1, q)\sigma_{n-2}Q(2n+1, q), \quad \text{for } n = 2, 4, 6, \dots,$$

$$(2.9) \quad DC_2^+(n, q) = \rho Q(2n+1, q)\sigma_{n-2}Q(2n+1, q), \quad \text{for } n = 2, 4, 6, \dots.$$

Then, from (2.5), we have:

$$(2.10) \quad |DC_i^\mp(n, q)| = A^\mp(n, q)B^\mp(n, q), \quad \text{for } i = 1, 2 \text{ (cf. (1.6)-(1.9))}.$$

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

3. Exponential sums over double cosets of $O(2n + 1, q)$

The following notations will be employed throughout this paper.

$$\begin{aligned} \text{tr}(x) &= x + x^3 + \dots + x^{3^{r-1}} \text{ the trace function } \mathbb{F}_q \rightarrow \mathbb{F}_3, \\ \lambda_0(x) &= e^{2\pi i x/3} \text{ the canonical additive character of } \mathbb{F}_3, \\ \lambda(x) &= e^{2\pi \text{tr}(x)/3} \text{ the canonical additive character of } \mathbb{F}_q. \end{aligned}$$

Then any nontrivial additive character ψ of \mathbb{F}_q is given by $\psi(x) = \lambda(ax)$, for a unique $a \in \mathbb{F}_q^*$. Also, since $\lambda(a)$ for any $a \in \mathbb{F}_q$ is a 3th root of 1, we have

$$(3.1) \quad \lambda(-a) = \lambda(2a) = \lambda(a)^2 = \lambda(a)^{-1} = \overline{\lambda(a)}.$$

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

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

Observe that, for $t = 1$, $K_{GL(1,q)}(\psi; a)$ denotes the Kloosterman sum $K(\psi; a)$. In [5], it is shown that $K_{GL(t,q)}(\psi; a)$ satisfies the following recursive relation: for integers $t \geq 2$, $a \in \mathbb{F}_q^*$,

$$K_{GL(t,q)}(\psi; a) = q^{t-1} K_{GL(t-1,q)}(\psi; a) K(\psi; a) + q^{2t-2} (q^{t-1} - 1) K_{GL(t-2,q)}(\psi; a),$$

where we understand that $K_{GL(0,q)}(\psi, a) = 1$.

Proposition 3.1. ([7]) *Let ψ be a nontrivial additive character of \mathbb{F}_q . For each positive integer r , let Ω_r be the set of all $r \times r$ nonsingular symmetric matrices over \mathbb{F}_q . Then we have*

$$(3.2) \quad a_r(\psi) = \sum_{B \in \Omega_r} \sum_{h \in \mathbb{F}_q^{r \times 1}} \psi({}^t h B h) = \begin{cases} q^{r(r+2)/4} \prod_{j=1}^{r/2} (q^{2j-1} - 1), & \text{for } r \text{ even,} \\ 0, & \text{for } r \text{ odd.} \end{cases}$$

From Sections 5 and 6 of [7] the Gauss sum for $O(2n+1, q)$, with ψ a nontrivial additive character of \mathbb{F}_q , is given by:

$$\sum_{w \in O(2n+1, q)} \psi(Trw) = \sum_{0 \leq r \leq n} \sum_{w \in Q\sigma_r Q} \psi(Trw) + \sum_{0 \leq r \leq n} \sum_{w \in \rho Q\sigma_r Q} \psi(Trw) \text{ (cf. (2.2))},$$

with

$$\begin{aligned} & \sum_{w \in Q\sigma_r Q} \psi(Trw) \\ (3.3) \quad &= |B_r \setminus Q| \sum_{w \in Q} \psi(Trw\sigma_r) \\ &= \psi(1)q^{\binom{n+1}{2}} |B_r \setminus Q| q^{r(n-r-1)} a_r(\psi) K_{GL(n-r, q)}(\psi; 1), \end{aligned}$$

$$\begin{aligned} & \sum_{w \in \rho Q\sigma_r Q} \psi(Trw) \\ (3.4) \quad &= |B_r \setminus Q| \sum_{w \in Q} \psi(Tr\rho w\sigma_r) \\ &= \psi(-1)q^{\binom{n+1}{2}} |B_r \setminus Q| q^{r(n-r-1)} a_r(\psi) K_{GL(n-r, q)}(\psi; 1). \end{aligned}$$

Here one uses (2.3) and the fact that $\rho^{-1}w\rho \in Q$, for all $w \in Q$.

We now see from (2.4) and (3.2)-(3.4) that, for each r with $0 \leq r \leq n$,

$$\begin{aligned} (3.5) \quad & \sum_{w \in Q\sigma_r Q} \psi(Trw) \\ &= \begin{cases} \psi(1)q^{\binom{n+1}{2}} q^{rn - \frac{1}{4}r^2} \begin{bmatrix} n \\ r \end{bmatrix}_q \prod_{j=1}^{r/2} (q^{2j-1} - 1) K_{GL(n-r, q)}(\psi; 1), & \text{if } r \text{ is even,} \\ 0, & \text{if } r \text{ is odd,} \end{cases} \end{aligned}$$

$$\begin{aligned} (3.6) \quad & \sum_{w \in \rho Q\sigma_r Q} \psi(Trw) \\ &= \begin{cases} \psi(-1)q^{\binom{n+1}{2}} q^{rn - \frac{1}{4}r^2} \begin{bmatrix} n \\ r \end{bmatrix}_q \prod_{j=1}^{r/2} (q^{2j-1} - 1) K_{GL(n-r, q)}(\psi; 1), & \text{if } r \text{ is even,} \\ 0, & \text{if } r \text{ is odd.} \end{cases} \end{aligned}$$

For our purposes, we need two infinite families of exponential sums in (3.5) over $DC_1^-(n, q)$, for $n = 1, 3, 5, \dots$, and over $DC_1^+(n, q)$, for $n = 2, 4, 6, \dots$. And also, we need two such sums in (3.6) over $DC_2^-(n, q)$, for $n = 1, 3, 5, \dots$, and over $DC_2^+(n, q)$, for $n = 2, 4, 6, \dots$. So we state them separately as a theorem.

Theorem 3.2. *Let ψ be any nontrivial additive character of \mathbb{F}_q . Then, in the notations of (1.6), (1.8), and (2.6)-(2.9), we have*

$$\begin{aligned}
 \sum_{w \in DC_1^-(n,q)} \psi(Trw) &= \psi(1)A^-(n, q)K(\psi; 1), \text{ for } n = 1, 3, 5, \dots, \\
 \sum_{w \in DC_2^-(n,q)} \psi(Trw) &= \psi(-1)A^-(n, q)K(\psi; 1), \text{ for } n = 1, 3, 5, \dots, \\
 \sum_{w \in DC_1^+(n,q)} \psi(Trw) &= \psi(1)q^{-1}A^+(n, q)K_{GL(2,q)}(\psi; 1) \\
 &= \psi(1)A^+(n, q)(K(\psi; 1)^2 + q^2 - q), \text{ for } n = 2, 4, 6, \dots, \\
 \sum_{w \in DC_2^+(n,q)} \psi(Trw) &= \psi(-1)q^{-1}A^+(n, q)K_{GL(2,q)}(\psi; 1) \\
 &= \psi(-1)A^+(n, q)(K(\psi; 1)^2 + q^2 - q), \text{ for } n = 2, 4, 6, \dots.
 \end{aligned}$$

The next corollary follows from Theorem 3.2 and simple changes of variables.

Corollary 3.3. *Let λ be the canonical additive character of \mathbb{F}_q , and let $a \in \mathbb{F}_q^*$. Then we have*

$$(3.7) \quad \sum_{w \in DC_1^-(n,q)} \lambda(aTrw) = \lambda(a)A^-(n, q)K(\lambda; a^2), \text{ for } n = 1, 3, 5, \dots,$$

$$(3.8) \quad \sum_{w \in DC_2^-(n,q)} \lambda(aTrw) = \lambda(-a)A^-(n, q)K(\lambda; a^2), \text{ for } n = 1, 3, 5, \dots,$$

$$(3.9) \quad \sum_{w \in DC_1^+(n,q)} \lambda(aTrw) = \lambda(a)A^+(n, q)(K(\lambda; a^2)^2 + q^2 - q), \text{ for } n = 2, 4, 6, \dots,$$

$$(3.10) \quad \sum_{w \in DC_2^+(n,q)} \lambda(aTrw) = \lambda(-a)A^+(n, q)(K(\lambda; a^2)^2 + q^2 - q), \text{ for } n = 2, 4, 6, \dots.$$

Proposition 3.4. ([5, (5.3-5)]) *Let λ be the canonical additive character of \mathbb{F}_q , $m \in \mathbb{Z}_{\geq 0}$, $\beta \in \mathbb{F}_q$. Then*

$$(3.11) \quad \sum_{a \in \mathbb{F}_q^*} \lambda(-a\beta)K(\lambda; a^2)^m = q\delta(m, q; \beta) - (q-1)^m,$$

where, for $m \geq 1$,

$$(3.12) \quad \delta(m, q; \beta) = |\{(\alpha_1, \dots, \alpha_m) \in (\mathbb{F}_q^*)^m \mid \alpha_1 + \alpha_1^{-1} + \dots + \alpha_m + \alpha_m^{-1} = \beta\}|,$$

and

$$(3.13) \quad \delta(0, q; \beta) = \begin{cases} 1, & \text{if } \beta = 0, \\ 0, & \text{otherwise.} \end{cases}$$

Remark 3.5. Here one notes that

$$(3.14) \quad \begin{aligned} \delta(1, q; \beta) &= |\{x \in \mathbb{F}_q \mid x^2 - \beta x + 1 = 0\}| \\ &= \begin{cases} 2, & \text{if } \beta^2 - 1 \neq 0 \text{ is a square,} \\ 1, & \text{if } \beta^2 - 1 = 0, \\ 0, & \text{if } \beta^2 - 1 \text{ is a nonsquare.} \end{cases} \end{aligned}$$

Lemma 3.6. ([13]) *Let $\delta(m, q; \beta)$ be as in (3.12) and (3.13), and let $a \in \mathbb{F}_q^*$. Then we have*

$$(3.15) \quad \sum_{\beta \in \mathbb{F}_q} \delta(m, q; \beta) \lambda(a\beta) = K(\lambda; a^2)^m.$$

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

$$\begin{aligned} N_{Q\sigma_r Q}(\beta) &= |\{w \in Q\sigma_r Q \mid Trw = \beta\}|, \\ N_{\rho Q\sigma_r Q}(\beta) &= |\{w \in \rho Q\sigma_r Q \mid Trw = \beta\}|. \end{aligned}$$

Then it is easy to see that

$$(3.16) \quad qN_{Q\sigma_r Q}(\beta) = |Q\sigma_r Q| + \sum_{a \in \mathbb{F}_q^*} \lambda(-a\beta) \sum_{w \in Q\sigma_r Q} \lambda(aTrw),$$

$$(3.17) \quad qN_{\rho Q\sigma_r Q}(\beta) = |\rho Q\sigma_r Q| + \sum_{a \in \mathbb{F}_q^*} \lambda(-a\beta) \sum_{w \in \rho Q\sigma_r Q} \lambda(aTrw).$$

Now, from (2.6)-(2.10) and (3.7)-(3.10), we have the following result.

Proposition 3.7. *With the notations of (1.6)-(1.9), we have:*

(1)

$$\begin{aligned} N_{DC_1^-(n, q)}(\beta) &= q^{-1}A^-(n, q)B^-(n, q) + q^{-1}A^-(n, q)(q\delta(1, q; \beta - 1) - q + 1) \\ &= q^{-1}A^-(n, q)B^-(n, q) + q^{-1}A^-(n, q) \end{aligned}$$

(3.18)

$$\times \begin{cases} q + 1, & \text{if } \beta^2 - 2\beta \neq 0 \text{ is a square,} \\ 1, & \text{if } \beta = 0 \text{ or } 2, \\ -q + 1, & \text{if } \beta^2 - 2\beta \text{ is a nonsquare,} \end{cases} \quad (\text{cf. (3.12), (3.14)})$$

(2)

$$\begin{aligned} N_{DC_2^-(n, q)}(\beta) &= q^{-1}A^-(n, q)B^-(n, q) + q^{-1}A^-(n, q)(q\delta(1, q; \beta + 1) - q + 1) \\ &= q^{-1}A^-(n, q)B^-(n, q) + q^{-1}A^-(n, q) \end{aligned}$$

$$(3.19) \quad \times \begin{cases} q+1, & \text{if } \beta^2 + 2\beta \neq 0 \text{ is a square,} \\ 1, & \text{if } \beta = 0 \text{ or } 1, \\ -q+1, & \text{if } \beta^2 + 2\beta \text{ is a nonsquare,} \end{cases}$$

(3)

(3.20)

$$N_{DC_1^+(n,q)}(\beta) = q^{-1}A^+(n,q)B^+(n,q) \\ + q^{-1}A^+(n,q) \times \begin{cases} q\delta(2,q;0) + (q-1)^3, & \text{if } \beta = 1, \\ q\delta(2,q;\beta-1) - 2q^2 + 3q - 1, & \text{if } \beta \neq 1, \end{cases}$$

(cf. (3.12))

(4)

(3.21)

$$N_{DC_2^+(n,q)}(\beta) = q^{-1}A^+(n,q)B^+(n,q) \\ + q^{-1}A^+(n,q) \times \begin{cases} q\delta(2,q;0) + (q-1)^3, & \text{if } \beta = -1, \\ q\delta(2,q;\beta+1) - 2q^2 + 3q - 1, & \text{if } \beta \neq -1. \end{cases}$$

Corollary 3.8. (1) For each odd integer $n \geq 3$, with all q , $N_{DC_1^-(n,q)}(\beta) > 0$, for all β ; for $n = 1$, with all q ,

$$(3.22) \quad N_{DC_1^-(n,q)}(\beta) = \begin{cases} 2q, & \text{if } \beta^2 - 2\beta \neq 0 \text{ is a square,} \\ q, & \text{if } \beta = 0 \text{ or } 2, \\ 0, & \text{if } \beta^2 - 2\beta \text{ is a nonsquare.} \end{cases}$$

(2) For each odd integer $n \geq 3$, with all q , $N_{DC_2^-(n,q)}(\beta) > 0$, for all β ; for $n = 1$, with all q ,

$$(3.23) \quad N_{DC_2^-(n,q)}(\beta) = \begin{cases} 2q, & \text{if } \beta^2 + 2\beta \neq 0 \text{ is a square,} \\ q, & \text{if } \beta = 0 \text{ or } 1, \\ 0, & \text{if } \beta^2 + 2\beta \text{ is a nonsquare.} \end{cases}$$

(3) For each even integer $n \geq 2$, with all q , $N_{DC_1^+(n,q)}(\beta) > 0$, for all β .

(4) For each even integer $n \geq 2$, with all q , $N_{DC_2^+(n,q)}(\beta) > 0$, for all β .

4. Construction of codes

Here we will construct two infinite families of ternary linear codes $C(DC_i^\mp(n,q))$ of length $A^\mp(n,q)B^\mp(n,q)$, associated with the double cosets $DC_i^\mp(n,q)$ ($i = 1, 2$).

Let

(4.1)

$$N_i^-(n,q) = |DC_i^-(n,q)| = A^-(n,q)B^-(n,q), \text{ for } i = 1, 2, \text{ and } n = 1, 3, 5, \dots,$$

(4.2)

$$N_i^+(n,q) = |DC_i^+(n,q)| = A^+(n,q)B^+(n,q), \text{ for } i = 1, 2, \text{ and } n = 2, 4, 6, \dots$$

(cf. (2.10)).

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

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

The ternary linear 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:

$$(4.3) \quad C(DC_i^\mp(n, q)) = \{u \in \mathbb{F}_2^{N_i^\mp(n, q)} \mid u \cdot v_i^\mp(n, q) = 0\}, \quad \text{for } i = 1, 2,$$

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

The following Delsarte's theorem is well-known.

Theorem 4.1. ([16]) *Let B be a linear code over \mathbb{F}_q . Then*

$$(B|_{\mathbb{F}_3})^\perp = tr(B^\perp).$$

In view of this theorem, the dual $C(DC_i^\mp(n, q))^\perp$ of the code $C(DC_i^\mp(n, q))$ is given by, for $i = 1, 2$,

$$(4.4) \quad C(DC_i^\mp(n, q))^\perp = \{c_i^\mp(a) = c_i^\mp(a; n, q) = (tr(aTrg_1), \dots, tr(aTrg_{N_i^\mp}(n, q))) \mid a \in \mathbb{F}_q\}.$$

Theorem 4.2. (1) *The map $\mathbb{F}_q \rightarrow C(DC_i^-(n, q))^\perp (a \mapsto c_i^-(a)) (i = 1, 2)$ is an \mathbb{F}_3 -linear isomorphism for each odd integer $n \geq 1$ and all q .*

(2) *The map $\mathbb{F}_q \rightarrow C(DC_i^+(n, q))^\perp (a \mapsto c_i^+(a)) (i = 1, 2)$ is an \mathbb{F}_3 -linear isomorphism for each even integer $n \geq 2$ and all q .*

Proof. All maps are clearly \mathbb{F}_3 -linear and surjective. Let a be in the kernel of map $\mathbb{F}_q \rightarrow C(DC_1^+(n, q))^\perp (a \mapsto c_1^+(a))$. Then $tr(aTrg) = 0$, for all $g \in DC_1^+(n, q)$. Since, by Corollary 3.8 (3), $Tr : DC_1^+(n, q) \rightarrow \mathbb{F}_q$ is surjective, and hence $tr(a\alpha) = 0$, for all $\alpha \in \mathbb{F}_q$. This implies that $a = 0$, since otherwise $tr : \mathbb{F}_q \rightarrow \mathbb{F}_3$ would be the zero map. This shows $i = 1$ case of (2). All the other assertions can be handled in the same way, except for $i = 1, 2$ and $n = 1$ case of (1), since in those cases the maps $Tr : DC_i^\mp(n, q) \rightarrow \mathbb{F}_q$ are surjective.

Let a be in the kernel of the map $\mathbb{F}_q \rightarrow C(DC_i^-(1, q))^\perp (a \mapsto c_i^-(a))$, for $i = 1, 2$. Then $tr(aTrg) = 0$, for all $g \in DC_i^-(1, q)$. Suppose that $a \neq 0$. Then we would have

$$\begin{aligned}
 q(q-1) &= |DC_i^-(1, q)| = \sum_{g \in DC_i^-(1, q)} e^{2\pi i \text{tr}(a \text{Tr}g)/3} \\
 &= \sum_{\beta \in \mathbb{F}_q} N_{DC_i^-(1, q)}(\beta) \lambda(a\beta) \\
 &= q \sum_{\beta \in \mathbb{F}_q} \delta(1, q; \beta \mp 1) \lambda(a\beta) \text{ (cf. (3.18), (3.19))} \\
 &= q \lambda(\pm a) \sum_{\beta \in \mathbb{F}_q} \delta(1, q; \beta \mp 1) \lambda(a(\beta \mp 1)) \\
 &= q \lambda(\pm a) \sum_{\beta \in \mathbb{F}_q} \delta(1, q; \beta) \lambda(a\beta) \\
 &= q \lambda(\pm a) K(\lambda; a^2) \text{ (cf. (3.15)).}
 \end{aligned}$$

Note here that it is $\beta - 1$, for $i = 1$, and $\beta + 1$, for $i = 2$. So, using Weil bound in (1.1), we would get

$$q - 1 = |K(\lambda; a^2)| \leq 2\sqrt{q}.$$

For $q \geq 9$, this is impossible. On the other hand, from (3.22) and (3.23) we see that, out of 6 elements in $DC_1^-(1, 3)$, 3 of them has $Tr = 0$ and 3 of them has $Tr = 2$; out of 6 elements in $DC_2^-(1, 3)$, 3 of them has $Tr = 0$ and 3 of them has $Tr = 1$. So in either case the kernel is trivial. \square

5. Power moments of Kloosterman sums with trace nonzero square arguments

Here we will be able to find, via Pless power moment identity, two infinite families of recursive formulas, the one generating the power moments of Kloosterman sums with trace nonzero square arguments and the other generating the even power moments of those.

Theorem 5.1. (Pless power moment identity, [16]) *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 $h = 0, 1, 2, \dots$,*

$$(5.1) \quad \sum_{j=0}^n j^h B_j = \sum_{j=0}^{\min\{n, h\}} (-1)^j B_j^\perp \sum_{t=j}^h t! S(h, t) q^{k-t} (q-1)^{t-j} \binom{n-j}{n-t},$$

where $S(h, t)$ is the Stirling number of the second kind defined in (1.14).

Lemma 5.2. *Let $c_i^\mp(a) = (\text{tr}(a \text{Tr}g_1), \dots, \text{tr}(a \text{Tr}g_{N_i^\mp(n, q)})) \in C(DC_i^\mp(n, q))^\perp$, for $a \in \mathbb{F}_q^*$, and $i = 1, 2$. Then the Hamming weights $w(c_i^\mp(a))$ are expressed as follows:*

$$\begin{aligned}
 (1) \quad & w(c_i^-(a)) \\
 (5.2) \quad & = \frac{2}{3} A^-(n, q) (B^-(n, q) - (\text{Re}\lambda(a)) K(\lambda; a^2)), \text{ for } i = 1, 2,
 \end{aligned}$$

$$\begin{aligned}
(2) \quad & w(c_i^+(a)) \\
(5.3) \quad & = \frac{2}{3}A^+(n, q)\{B^+(n, q) - (Re\lambda(a))(K(\lambda; a^2)^2 + q^2 - q)\}, \text{ for } i = 1, 2.
\end{aligned}$$

Proof.

$$\begin{aligned}
(5.4) \quad w(c_i^\mp(a)) &= \sum_{j=1}^{N_i^\mp(n, q)} \left(1 - \frac{1}{3} \sum_{\alpha \in \mathbb{F}_3} \lambda_0(\alpha \text{Tr}(a \text{Tr} g_j))\right) \\
&= N_i^\mp(n, q) - \frac{1}{3} \sum_{\alpha \in \mathbb{F}_3} \sum_{w \in DC_i^\mp(n, q)} \lambda(\alpha a \text{Tr} w) \\
&= \frac{2}{3}N_i^\mp(n, q) - \frac{1}{3} \sum_{\alpha \in \mathbb{F}_3^*} \sum_{w \in DC_i^\mp(n, q)} \lambda(\alpha a \text{Tr} w).
\end{aligned}$$

Now, the results follow from (3.7), (3.10), (4.1), and (4.2). \square

Let $u = (u_1, \dots, u_{N_i^\mp(n, q)}) \in \mathbb{F}_3^{N_i^\mp(n, q)}$, with ν_β 1's and μ_β 2's in the coordinate places where $\text{Tr}(g_j) = \beta$, for each $\beta \in \mathbb{F}_q$. Then we see from the definition of the code $C(DC_i^\mp(n, q))$ (cf. (4.3)) that u is a codeword with weight j if and only if $\sum_{\beta \in \mathbb{F}_q} \nu_\beta + \sum_{\beta \in \mathbb{F}_q} \mu_\beta = j$ and $\sum_{\beta \in \mathbb{F}_q} \nu_\beta \beta = \sum_{\beta \in \mathbb{F}_q} \mu_\beta \beta$ (an identity in \mathbb{F}_q). Note that there are $\prod_{\beta \in \mathbb{F}_q} \binom{N_{DC_i^\mp(n, q)}(\beta)}{\nu_\beta, \mu_\beta}$ (cf. (1.4), (1.5)) many such codewords with weight j . Now, we get the following formulas in (5.5)-(5.8), by using the explicit values of $N_{DC_i^\mp(n, q)}(\beta)$ in (3.18)-(3.21) (cf. (1.6)-(1.9)).

Theorem 5.3. *Let $\{C_{i,j}^\mp(n, q)\}_{j=0}^{N_i^\mp(n, q)}$ be the weight distribution of $C(DC_i^\mp(n, q))$, for $i = 1, 2$. Then we have:*

(1) For $j = 0, \dots, N_1^-(n, q)$,

$$\begin{aligned}
(5.5) \quad C_{1,j}^-(n, q) &= \sum_{\beta \in \mathbb{F}_q} \prod_{\beta \in \mathbb{F}_q} \binom{q^{-1}A^-(n, q)(B^-(n, q) + q\delta(1, q; \beta - 1) - q + 1)}{\nu_\beta, \mu_\beta} \\
&= \sum \binom{q^{-1}A^-(n, q)(B^-(n, q) + 1)}{\nu_0, \mu_0} \binom{q^{-1}A^-(n, q)(B^-(n, q) + 1)}{\nu_2, \mu_2} \\
&\quad \times \prod_{\beta^2 - 2\beta \neq 0 \text{ square}} \binom{q^{-1}A^-(n, q)(B^-(n, q) + q + 1)}{\nu_\beta, \mu_\beta} \\
&\quad \times \prod_{\beta^2 - 2\beta \text{ nonsquare}} \binom{q^{-1}A^-(n, q)(B^-(n, q) - q + 1)}{\nu_\beta, \mu_\beta},
\end{aligned}$$

(2) For $j = 0, \dots, N_2^-(n, q)$,

$$\begin{aligned}
 C_{2,j}^-(n, q) &= \sum_{\beta \in \mathbb{F}_q} \prod_{\beta \in \mathbb{F}_q} \binom{q^{-1}A^-(n, q)(B^-(n, q) + q\delta(1, q; \beta + 1) - q + 1)}{\nu_\beta, \mu_\beta} \\
 (5.6) \quad &= \sum \binom{q^{-1}A^-(n, q)(B^-(n, q) + 1)}{\nu_0, \mu_0} \binom{q^{-1}A^-(n, q)(B^-(n, q) + 1)}{\nu_1, \mu_1} \\
 &\times \prod_{\beta^2 + 2\beta \neq 0 \text{ square}} \binom{q^{-1}A^-(n, q)(B^-(n, q) + q + 1)}{\nu_\beta, \mu_\beta} \\
 &\times \prod_{\beta^2 + 2\beta \text{ nonsquare}} \binom{q^{-1}A^-(n, q)(B^-(n, q) - q + 1)}{\nu_\beta, \mu_\beta} \text{ (cf. (3.12), (3.14))},
 \end{aligned}$$

(3) For $j = 0, \dots, N_1^+(n, q)$,

$$\begin{aligned}
 C_{1,j}^+(n, q) &= \sum \binom{q^{-1}A^+(n, q)(B^+(n, q) + q\delta(2, q; 0) + (q-1)^3)}{\nu_1, \mu_1} \\
 (5.7) \quad &\times \prod_{\beta \neq 1} \binom{q^{-1}A^+(n, q)(B^+(n, q) + q\delta(2, q; \beta - 1) - 2q^2 + 3q - 1)}{\nu_\beta, \mu_\beta},
 \end{aligned}$$

(4) For $j = 0, \dots, N_2^+(n, q)$,

$$\begin{aligned}
 C_{2,j}^+(n, q) &= \sum \binom{q^{-1}A^+(n, q)(B^+(n, q) + q\delta(2, q; 0) + (q-1)^3)}{\nu_{-1}, \mu_{-1}} \\
 (5.8) \quad &\times \prod_{\beta \neq -1} \binom{q^{-1}A^+(n, q)(B^+(n, q) + q\delta(2, q; \beta + 1) - 2q^2 + 3q - 1)}{\nu_\beta, \mu_\beta}
 \end{aligned}$$

(cf. (3.12)),

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

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

Theorem 5.4. ([8]) (1) For each odd $n \geq 1$ and all q , and $h = 1, 2, 3, \dots$,

(5.9)

$$\begin{aligned}
 &2\left(\frac{2}{3}\right)^h A^-(n, q)^h \sum_{j=0}^h (-1)^j \binom{h}{j} B^-(n, q)^{h-j} S K^j \\
 &= q \sum_{j=0}^{\min\{N_i^-(n, q), h\}} (-1)^j C_j^-(n, q) \sum_{t=j}^h t! S(h, t) 3^{-t} 2^{t-j} \binom{N_i^-(n, q) - j}{N_i^-(n, q) - t},
 \end{aligned}$$

where $N_i^-(n, q) = |DC_i^-(n, q)| = A^-(n, q)B^-(n, q)$, $S(h, t)$ indicates the Stirling number of the second kind as in (1.14), and $\{C_j^-(n, q)\}_{j=0}^{N_i^-(n, q)}$ denotes the weight distribution of $C(DC^-(n, q))$ given by

$$\begin{aligned} C_j^-(n, q) &= \sum \binom{q^{-1}A^-(n, q)(B^-(n, q) + 1)}{\nu_1, \mu_1} \binom{q^{-1}A^-(n, q)(B^-(n, q) + 1)}{\nu_{-1}, \mu_{-1}} \\ &\times \prod_{\beta^2 - 1 \neq 0 \text{ square}} \binom{q^{-1}A^-(n, q)(B^-(n, q) + q + 1)}{\nu_\beta, \mu_\beta} \\ &\times \prod_{\beta^2 - 1 \text{ nonsquare}} \binom{q^{-1}A^-(n, q)(B^-(n, q) - q + 1)}{\nu_\beta, \mu_\beta} \quad (j = 0, \dots, N_i^-(n, q)). \end{aligned}$$

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

(2) For each even $n \geq 2$ and all q , and $h = 1, 2, 3, \dots$,

(5.10)

$$\begin{aligned} &2\left(\frac{2}{3}\right)^h A^+(n, q)^h \sum_{j=0}^h (-1)^j \binom{h}{j} (B^+(n, q) - q^2 + q)^{h-j} SK^{2j} \\ &= q \sum_{j=0}^{\min\{N_i^+(n, q), h\}} (-1)^j C_j^+(n, q) \sum_{t=j}^h t! S(h, t) 3^{-t} 2^{t-j} \binom{N_i^+(n, q) - j}{N_i^+(n, q) - t}, \end{aligned}$$

where $N_i^+(n, q) = |DC_i^+(n, q)| = A^+(n, q)B^+(n, q)$, and $\{C_j^+(n, q)\}_{j=0}^{N_i^+(n, q)}$ is the weight distribution of $C(DC^+(n, q))$ given by

$$\begin{aligned} C_j^+(n, q) &= \sum \binom{q^4(\delta(2, q; 0) + q^5 - q^2 - 3q + 3)}{\nu_0, \mu_0} \\ &\times \prod_{\beta \in \mathbb{F}_q^*} \binom{q^4(\delta(2, q; \beta) + q^5 - q^3 - q^2 - 2q + 3)}{\nu_\beta, \mu_\beta} \quad (j = 0, \dots, N_i^+(n, q)). \end{aligned}$$

Here the sum is over all the sets of nonnegative integers $\{\nu_\beta\}_{\beta \in \mathbb{F}_q}$ and $\{\mu_\beta\}_{\beta \in \mathbb{F}_q}$ satisfying $\sum_{\beta \in \mathbb{F}_q} \nu_\beta + \sum_{\beta \in \mathbb{F}_q} \mu_\beta = j$, and $\sum_{\beta \in \mathbb{F}_q} \nu_\beta \beta = \sum_{\beta \in \mathbb{F}_q} \mu_\beta \beta$, and, for every $\beta \in \mathbb{F}_q$,

$$\delta(2, q; \beta) = |\{(\alpha_1, \alpha_2) \in (\mathbb{F}_q^*)^2 \mid \alpha_1 + \alpha_1^{-1} + \alpha_2 + \alpha_2^{-1} = \beta\}|.$$

Remark 5.5. In [8], Theorem 5.4 (1) above is stated to hold for each odd $n \geq 3$ and all q , but it is also true for $n = 1$ and all q . Indeed, this can be shown by employing the same method as was done in the proof of Theorem 4.2.

We are now ready to apply the Pless power moment identity in (5.1) to $C(DC_i^\mp(n, q))^\perp$, for $i = 1, 2$, in order to obtain the results in Theorem 1.1 (cf. (1.10)-(1.13), (1.15)-(1.18)) about recursive formulas. The left hand side of that identity in (5.1) is equal to

$$(5.11) \quad \sum_{a \in \mathbb{F}_q^*} w(c_i^\mp(a))^h,$$

with the $w(c_i^\mp(a))$ given by (5.2) and (5.3). We do this for $w(c_i^-(a))$. In below, “the sum over $tra = 0$ (resp. $tra \neq 0$) ” will mean “the sum over all $a \in \mathbb{F}_q^*$, with $tra = 0$ (resp. $tra \neq 0$).”

$$(5.12) \quad \begin{aligned} \sum_{a \in \mathbb{F}_q^*} w(c_i^-(a))^h &= \left(\frac{2}{3}\right)^h A^-(n, q)^h \sum_{a \in \mathbb{F}_q^*} (B^-(n, q) - (Re\lambda(a))K(\lambda; a^2))^h \\ &= \left(\frac{2}{3}\right)^h A^-(n, q)^h \sum_{tra=0} (B^-(n, q) - K(\lambda; a^2))^h \\ &\quad + \left(\frac{2}{3}\right)^h A^-(n, q)^h \sum_{tra \neq 0} (B^-(n, q) + \frac{1}{2}K(\lambda; a^2))^h \end{aligned}$$

(nothing that $Re\lambda(a) = 1$, if $tra = 0$; $Re\lambda(a) = -\frac{1}{2}$, if $tra \neq 0$, i.e., $tra = 1, 2$)

$$\begin{aligned} &= \left(\frac{2}{3}\right)^h A^-(n, q)^h \sum_{tra=0} \sum_{j=0}^h (-1)^j \binom{h}{j} B^-(n, q)^{h-j} K(\lambda; a^2)^j \\ &\quad + \left(\frac{2}{3}\right)^h A^-(n, q)^h \sum_{tra \neq 0} \sum_{j=0}^h \binom{h}{j} B^-(n, q)^{h-j} 2^{-j} K(\lambda; a^2)^j \\ &= \left(\frac{2}{3}\right)^h A^-(n, q)^h \sum_{j=0}^h (-1)^j \binom{h}{j} B^-(n, q)^{h-j} (2SK^j - T_{12}SK^j) \text{ (cf. (1.1), (1.2))} \\ &\quad + \left(\frac{2}{3}\right)^h A^-(n, q)^h \sum_{j=0}^h \binom{h}{j} B^-(n, q)^{h-j} 2^{-j} T_{12}SK^j \\ &= 2\left(\frac{2}{3}\right)^h A^-(n, q)^h \sum_{j=0}^h (-1)^j \binom{h}{j} B^-(n, q)^{h-j} SK^j \\ &\quad + \left(\frac{2}{3}\right)^h A^-(n, q)^h \sum_{j=1}^h ((-1)^{j+1} + 2^{-j}) \binom{h}{j} B^-(n, q)^{h-j} T_{12}SK^j \end{aligned}$$

$$\begin{aligned}
&= q \sum_{j=0}^{\min\{N_i^-(n,q),h\}} (-1)^j C_j^-(n,q) \sum_{t=j}^h t! S(h,t) 3^{-t} 2^{t-j} \binom{N_i^-(n,q)-j}{N_i^-(n,q)-t} \quad (\text{from (5.9)}) \\
&\quad + \left(\frac{2}{3}\right)^h A^-(n,q)^h \sum_{j=1}^h ((-1)^{j+1} + 2^{-j}) \binom{h}{j} B^-(n,q)^{h-j} T_{12} S K^j.
\end{aligned}$$

Similarly,

(5.13)

$$\begin{aligned}
\sum_{a \in \mathbb{F}_q^*} w(c_i^+(a))^h &= 2 \left(\frac{2}{3}\right)^h A^+(n,q)^h \sum_{j=0}^h (-1)^j \binom{h}{j} (B^+(n,q) - q^2 + q)^{h-j} S K^{2j} \\
&\quad + \left(\frac{2}{3}\right)^h A^+(n,q)^h \sum_{j=0}^h \binom{h}{j} \{(-1)^{j+1} (B^+(n,q) - q^2 + q)^{h-j} \\
&\quad + 2^{-j} (B^+(n,q) + \frac{1}{2}q^2 - \frac{1}{2}q)^{h-j}\} T_{12} S K^{2j} \\
&= q \sum_{j=0}^{\min\{N_i^+(n,q),h\}} (-1)^j C_j^+(n,q) \sum_{t=j}^h t! S(h,t) 3^{-t} 2^{t-j} \binom{N_i^+(n,q)-j}{N_i^+(n,q)-t} \\
&\quad + \left(\frac{2}{3}\right)^h A^+(n,q)^h \sum_{j=0}^h \binom{h}{j} \{(-1)^{j+1} (B^+(n,q) - q^2 + q)^{h-j} \\
&\quad + 2^{-j} (B^+(n,q) + \frac{1}{2}q^2 - \frac{1}{2}q)^{h-j}\} T_{12} S K^{2j} \quad (\text{from (5.10)}).
\end{aligned}$$

On the other hand, the right hand side of (5.1) is

$$(5.14) \quad q \sum_{j=0}^{\min\{N_i^\mp(n,q),h\}} (-1)^j C_{i,j}^\mp(n,q) \sum_{t=j}^h t! S(h,t) 3^{-t} 2^{t-j} \binom{N_i^\mp(n,q)-j}{N_i^\mp(n,q)-t}.$$

Here one has to note that $\dim_{\mathbb{F}_3} C(DC_i^\mp(n,q)) = r$ (cf. Theorem 4.2) and to separate the terms corresponding to $j = h$ of the second sums in (5.12) and (5.13). Our main results in Theorem 1.1 now follow by equating either (5.12) or (5.13) with (5.14).

REFERENCES

- [1] R.J. Evans, *Seventh power moments of Kloosterman sums*, Israel J. Math. **175**, 349-362, 2010.
- [2] G. van der Geer, R. Schoof and M. van der Vlugt, *Weight formulas for ternary Melas codes*, Math. Comp. **58**, 781-792, 1992.
- [3] K. Hulek, J. Spandaw, B. van Geemen, D. van Straten, *The modularity of the Barth-Nieto quintic and its relatives*, Adv. Geom. **1**, 263-289, 2001.

- [4] N.E. Hurt, *Exponential Sums and Coding Theory: A Review* Acta Appl. Math. **46**, 49-91, 1997.
- [5] D. S. Kim, *Gauss sums for symplectic groups over a finite field*, Mh. Math. **126**, 55-71, 1998.
- [6] D. S. Kim, *Exponential sums for symplectic groups and their applications*, Acta Arith **88**, 155-171, 1999.
- [7] D. S. Kim, *Gauss sums for $O(2n + 1, q)$* , Finite Fields Appl. **4**, 62-86, 1998.
- [8] 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**, 167-178, 2009.
- [9] D. S. Kim, *Ternary codes associated with $O(3, 3^r)$ and power moments of Kloosterman sums with trace nonzero square arguments*, Math. Commun. **17**, 241-255, 2012.
- [10] D. S. Kim, *Infinite families of recursive formulas generating power moments of ternary Kloosterman sums with square arguments associated with $O^-(2n, q)$* , J. Korean Math. Soc. **48 (2)**, 267-288, 2011.
- [11] D. S. Kim, *Recursive formulas generating power moments of Kloosterman sums: symplectic case*, Montes Taurus J. Pure Appl. Math. **1 (1)**, 77-95, 2019.
- [12] J.-Y. Kim, S.-T. Choi, J.-S. No, H. Chung, *A New Family of p -ary Decimated Sequences with Low Correlation* in Proc. of IEEE Int. Symp. Information Theory (ISIT2010) - Austin, TX, 1263-1267, 2010.
- [13] H. D. Kloosterman, *On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$* , Acta Math. **49**, 407-464, 1926.
- [14] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl. 20, Cambridge University Press, Cambridge, 1987.
- [15] R. Livné, *Motivic orthogonal two-dimensional representations of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$* , Israel J. Math. **92**, 149-156, 1995.
- [16] F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error Correcting Codes*, North-Holland, Amsterdam, 1998.
- [17] M. Moisisio, *On the moments of Kloosterman sums and fibre products of Kloosterman curves*, Finite Fields Appl. **14**, 515-531, 2008.
- [18] K. G. Paterson, *Applications of Exponential Sums in Communications Theory, in Cryptography and Coding*, 1-24, Michael Walker, ed., LNCS Vol. 1746, Springer, 1999.
- [19] C. Peters, J. Top, 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**, 151-176, 1992.
- [20] H. Salié, *Über die Kloostermanschen Summen $S(u, v; q)$* , Math. Z. **34** 91-109, 1931.

(Dae San Kim) DEPARTMENT OF MATHEMATICS, SOGANG UNIVERSITY, SEOUL 121-742, KOREA

E-mail address: dskim@sogang.ac.kr