TERNARY CODES ASSOCIATED WITH $O^{-}(2n, q)$ AND POWER MOMENTS OF KLOOSTERMAN SUMS WITH SQUARE ARGUMENTS

Dae San Kim

Department of Mathematics, Sogang University, Seoul 121-742, Republic of Korea
(e-mail: dskim@sogang.ac.kr)

Received October 24, 2010

Abstract. In this paper, we construct three ternary linear codes associated with the orthogonal group $O^{-}(2, q)$ and the special orthogonal groups $SO^{-}(2, q)$ and $SO^{-}(4, q)$. Here $q$ is a power of three. Then we obtain 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 the codes. This is done via Pless power moment identity and by utilizing the explicit expressions of “Gauss sums” for the orthogonal and special orthogonal groups $O^{-}(2n, q)$ and $SO^{-}(2n, q)$.

MSC: 11T23, 20G40, 94B05

Keywords: ternary linear code, power moment, Kloosterman sum, square argument, Pless power moment identity, Gauss sum, orthogonal group, weight distribution

1 INTRODUCTION

Let $\psi$ be a nontrivial additive character of the finite field $\mathbb{F}_q$ with $q = p^r$ elements ($p$ a prime). Then the Kloosterman sum $K(\psi; a)$ (see [11]) is defined by

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

For this, we have the Weil bound

$$|K(\psi; a)| \leq 2\sqrt{q}. \quad (1.1)$$

The Kloosterman sum was introduced in 1926 (see [10]) to give an estimate for the Fourier coefficients of modular forms.

* This work was supported by the National Research Foundation of Korea grant funded by the Korean Government 2009-0072514.
For each nonnegative integer \( h \), by \( MK(\psi)^h \) we will denote the \( h \)th moment of the Kloosterman sum \( K(\psi; a) \). 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 we simply denote \( MK(\lambda)^h \) by \( MK^h \).

Also, we introduce incomplete power moments of Kloosterman sums. Namely, for every nonnegative integer \( h \) and \( \psi \) as before, we define

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

which is called the \( h \)th moment of Kloosterman sums with “square arguments.” If \( \psi = \lambda \) is the canonical additive character of \( \mathbb{F}_q \), then, for short, we denote \( SK(\lambda)^h \) by \( SK^h \).

Explicit computations on power moments of Kloosterman sums were begun in 1931 by Salié [16], who showed that, for any odd prime \( q \),

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

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

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

For \( q = p \) odd prime, Salié [16] obtained \( MK^1, MK^2, MK^3, MK^4 \) 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 \( \Gamma_0(15) \) (see [12, 15]). \( MK^6 \) can be expressed in terms of the \( p \)th eigenvalue for a weight-4 newform on \( \Gamma_0(6) \) (see [3]).

Also, based on the numerical evidence, Evans [1] proposed 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.

Assume now that \( q = 3^r \). Recently, Moisio [14] was able to find explicit expressions of \( MK^h \) for \( h \leq 10 \). 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 \( q - 1 \) that were known by the work of Geer, Schoof, and Vlugt [2]. In this paper, we are be able to produce three recursive formulas generating power moments of Kloosterman sums with square arguments over finite fields of characteristic three. To do that, we will construct three ternary linear codes \( C(SO^-(2, q)) \), \( C(O^-(2, q)) \), and \( C(SO^-(4, q)) \), respectively, associated with \( SO^-(2, q), O^-(2, q) \), and \( SO^-(4, q) \), and express those power moments in terms of the frequencies of weights in each code. Then, thanks to our previous results on explicit expressions of “Gauss sums” for the orthogonal and special orthogonal groups \( O^-(2n, q) \) and \( SO^-(2n, q) \), we can express the weight of each codeword in the duals of the codes in terms of Kloosterman sums with square arguments. Then our formulas will follow immediately from the Pless power moment identity (see (5.1)). Similar results of this paper were obtained in [9] for the case of finite symplectic groups over finite fields of characteristic three. Also, in the same case, infinite families of recursive formulas were derived in [8] by using explicit expressions of exponential sums associated with certain double cosets.

The main result of this paper Theorem 1 below (see (1.5), (1.6), (1.8)–(1.12)). Henceforth, we agree that, for nonnegative integers \( a, b, c \),

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