Bull. Aust. Math. Soc. **79** (2009), 427–435
doi:10.1017/S0004972708001366

CODES ASSOCIATED WITH $Sp(4, q)$ AND EVEN-POWER MOMENTS OF KLOOSTERMAN SUMS

JI HYUN KIM

(Received 31 July 2008)

Abstract

Here we derive a recursive formula for even-power moments of Kloosterman sums or equivalently for power moments of two-dimensional Kloosterman sums. This is done by using the Pless power-moment identity and an explicit expression of the Gauss sum for $Sp(4, q)$.

2000 *Mathematics subject classification*: primary 94A24, 11L05.

Keywords and phrases: linear code, symplectic group, Gauss sum, Kloosterman sum, Pless power moment identity, weight distribution.

1. Introduction

Let χ_1 be the canonical additive character of the finite field $\mathbb{F}_q$ with $q = 2^r$, and let m be a positive integer.

The m-dimensional Kloosterman [7] sum $K_m(a)$ is given by

$$K_m(a) = K_m(\chi_1; a) = \sum_{x_1,\ldots,x_m \in \mathbb{F}_q^*} \chi_1(x_1 + \cdots + x_m + a x_1^{-1} \cdots x_m^{-1}) \quad (a \in \mathbb{F}_q^*).$$

In particular, if $m = 1$, then $K_1(a) := K(a)$ is called the Kloosterman sum. The Kloosterman [5] sum was introduced in 1926 to give an estimate for the Fourier coefficients of modular forms.

Let h be a nonnegative integer, and let

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

denote the hth moment of the m-dimensional Kloosterman sum $K_m(a)$. Furthermore, MK_1^h is simply denoted by MK^h. The power moments of Kloosterman sums over

This work was supported by grant No. R01-2006-000-11176-0 from the Basic Research Program of the Korea Science and Engineering Foundation.

finite fields of characteristic 2 have been studied in an estimate for the Kloosterman sums and have been used in solving a variety of problems from coding theory.

Carlitz obtained MK^h for $h \leq 4$ in [1], and Moisio computed MK^6 in [11]. Lately, Moisio [9] evaluated MK^h, for $h \leq 10$, 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 Van der Vlugt in [12].

In this paper, we adopt Moisio's idea to show the following theorem giving a recursive formula for the even-power moments of Kloosterman sums. To do that, we construct the codes $C(Sp(4, q))$ associated with finite symplectic groups $Sp(4, q)$, and express the power moments in terms of the frequencies of weights in the code. We could construct the codes $C(Sp(2, q))$ associated with $Sp(2, q) = SL(2, q)$ and get a recursive formula producing power moments of Kloosterman sums. But this case has been treated already in [4].

Thanks to the previous result on the explicit expression of 'Gauss sum' for the symplectic groups (see [3]), we can represent the weight of each codeword in the dual $C^{\perp}(Sp(4, q))$ of $C(Sp(4, q))$ in terms of two-dimensional Kloosterman sums. Then we get the following recursive formula from the Pless power-moment identity.

THEOREM 1.1. *For any positive integer h, the even-power moments MK^{2h} of the Kloosterman sum $K(a)$ are given by*

$$q^{4h} MK^{2h} = \sum_{i=0}^{h-1} (-1)^{i+h+1} \binom{h}{i} (N - q^7 + q^5)^{h-i} q^{4i} MK^{2i} + q \sum_{i=0}^{\min\{N,h\}} (-1)^{i+h} C_i \sum_{t=i}^{h} t! S(h, t) 2^{h-t} \binom{N-i}{N-t}.$$

Here

$$N = |Sp(4, q)| = q^4(q^2 - 1)(q^4 - 1), \tag{1.1}$$

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

$$S(h, t) = \frac{1}{t!} \sum_{j=0}^{t} (-1)^{t-j} \binom{t}{j} j^h. \tag{1.2}$$

In addition, $\{C_i\}_{i=0}^N$ denotes the weight distribution of the code $C = C(Sp(4, q))$ given by

$$C_i = \sum \binom{q^9 - q^6 - q^5}{\nu_0} \prod_{\beta \in \mathbb{F}_q^*} \binom{n_\beta}{\nu_\beta}, \tag{1.3}$$

where $n_\beta = q^4 K(\chi_1; \beta^{-1}) + q^9 - q^7 - q^6 - q^5$ and the sum runs over all the set of nonnegative integers $\{\nu_\beta\}_{\beta \in \mathbb{F}_q}$ satisfying $\sum_{\beta \in \mathbb{F}_q} \nu_\beta = i$ and $\sum_{\beta \in \mathbb{F}_q} \nu_\beta \beta = 0$ (an identity in $\mathbb{F}_q$).

We obtain an alternative recursive formula from Carlitz [2, Theorem 2.6].

https://doi.org/10.1017/S0004972708001366 Published online by Cambridge University Press

COROLLARY 1.2. *For any positive integer h, we have the following recursive formula for the moments MK_2^h of the two-dimensional Kloosterman sums,*

$$q^{4h}MK_2^h = \sum_{i=0}^{h-1}(-1)^{i+h+1}\binom{h}{i}(N-q^7)^{h-i}q^{4i}MK_2^i + q\sum_{i=0}^{\min\{N,h\}}(-1)^{i+h}C_i\sum_{t=i}^{h}t!S(h,t)2^{h-t}\binom{N-i}{N-t}$$

where C_i is the weight distribution of the code $C = C(Sp(4, q))$ given by (1.3), and $S(h, t)$ indicates the Stirling number of the second kind given by (1.2).

2. Preliminaries

The following notation will be used throughout this paper:

(i) $q = 2^r\,(r \in \mathbb{Z}_{>0})$;
(ii) $Sp(2n, q)$ = the symplectic group over $\mathbb{F}_q$ defined by
$\{g \in GL(2n, q) \mid {}^t gJg = J\}$, with $J = \left[\begin{smallmatrix} 0 & I_n \\ -I_n & 0 \end{smallmatrix}\right]$;
(iii) $N = q^{n^2}\prod_{j=1}^{n}(q^{2j}-1)$ the order of $Sp(2n, q)$;
(iv) $\mathrm{Tr}(g)$ = the matrix trace for $g \in Sp(2n, q)$;
(v) $tr(x) = x + x^2 + \cdots + x^{2^{r-1}}$ the trace function $\mathbb{F}_q \to \mathbb{F}_2$;
(vi) $\chi_1(x) = (-1)^{tr(x)}$ the canonical additive character of $\mathbb{F}_q$;
(vii) $\chi_a(x) = \chi_1(ax)$ an additive character of $\mathbb{F}_q$ $(a \in \mathbb{F}_q)$.

Let $g_1, g_2, \ldots, g_N$ be a fixed ordering of the elements in $Sp(4, q)$. Let $C = C(Sp(4, q))$ be the binary linear code of length N defined by

$$C = \{u \in \mathbb{F}_2^N \mid u \cdot v = 0\},$$

where $v = (\mathrm{Tr}(g_1), \ldots, \mathrm{Tr}(g_N)) \in \mathbb{F}_q^N$.

THEOREM 2.1 (Delsarte [8]). *Let B be a linear code over $\mathbb{F}_q$, then*

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

From Delsarte's theorem, the next result follows immediately.

THEOREM 2.2. *The dual $C^{\perp} = C^{\perp}(Sp(4, q))$ of $C = C(Sp(4, q))$ is given by*

$$C^{\perp} = \{c(a) = (tr(a\mathrm{Tr}(g_1)), \ldots, tr(a\mathrm{Tr}(g_N))) \mid a \in \mathbb{F}_q\}.$$

We need the next theorem about the Gauss sum for $Sp(2n, q)$.

THEOREM 2.3 (Kim [3]). *For any nontrivial additive character $\chi_a(a \in \mathbb{F}_q^*)$ of $\mathbb{F}_q$, the Gauss sum over $Sp(2n, q)$*

$$\sum_{g \in Sp(2n,q)} \chi_a(\mathrm{Tr}(g))$$

https://doi.org/10.1017/S0004972708001366 Published online by Cambridge University Press

is given by

$$q^{n^2-1}\sum_{r=0}^{[n/2]} q^{r(r+1)}\begin{bmatrix} n\\ r\end{bmatrix}_q \prod_{i=1}^{r}(q^{2i-1}-1)\sum_{l=1}^{[(n-2r+2)/2]} q^l K(\chi_a;\, 1)^{n-2r+2-2l}$$
$$\times \sum \prod_{\nu=1}^{l-1}(q^{j_\nu}-1)$$

where the innermost sum is over all integers $j_1, \ldots, j_{l-1}$ *satisfying* $2l-3 \le j_1 \le n-2r-1$, $2l-5 \le j_2 \le j_1-2, \ldots, 1 \le j_{l-1} \le j_{l-2}-2$.

Here, for integers n, r *with* $0 \le r \le n$, *the* q*-binomial coefficients are given by*

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

We need the case, $n = 2$, of Theorem 2.3.

COROLLARY 2.4. *For any* $a \in \mathbb{F}_q^*$,

$$\sum_{g\in Sp(4,q)} \chi_a(\mathrm{Tr}(g)) = q^4\{K(\chi_a;\, 1)^2 + q^3 - q\}. \tag{2.1}$$

The following result is easy to verify.

LEMMA 2.5. *For any* $a \in \mathbb{F}_q^*$, *the Kloosterman sum* $K(\chi_a;\, 1)$ *is equal to* $K(\chi_1;\, a)$.

THEOREM 2.6 (Carlitz [2]).

$$K_2(\chi_1;\, a) = K(\chi_1;\, a)^2 - q.$$

So, from Lemma 2.5 and Theorem 2.6, we have the following alternative description of (2.1).

COROLLARY 2.7. *For any* $a \in \mathbb{F}_q^*$,

$$\sum_{g\in Sp(4,q)} \chi_a(\mathrm{Tr}(g)) = q^4\{K(\chi_1;\, a)^2 + q^3 - q\} \tag{2.2}$$
$$= q^4\{K_2(\chi_1;\, a) + q^3\}. \tag{2.3}$$

PROPOSITION 2.8. *For* $\beta \in \mathbb{F}_q^*$,

$$\sum_{a\in\mathbb{F}_q^*} \chi_1(-a\beta) \sum_{g\in Sp(4,q)} \chi_1(a\mathrm{Tr}\, g) \tag{2.4}$$
$$= \begin{cases} q^8 - q^7 - q^4 & \text{if } \beta = 0,\\ q^5 K(\chi_1;\, \beta^{-1}) - q^7 - q^4 & \text{if } \beta \ne 0.\end{cases} \tag{2.5}$$

https://doi.org/10.1017/S0004972708001366 Published online by Cambridge University Press

PROOF. Using (2.3), (2.4) is equal to

$$\begin{aligned}
&q^4 \sum_{a\in\mathbb{F}_q^*} \chi_1(-a\beta)\{K_2(\chi_1; a) + q^3\} \\
&= q^4 \sum_{a\in\mathbb{F}_q^*} \chi_1(-a\beta) K_2(\chi_1; a) + q^7 \sum_{a\in\mathbb{F}_q^*} \chi_1(-a\beta) \\
&= q^4 \Big\{ \sum_{a\in\mathbb{F}_q^*} \chi_1(-a\beta) \sum_{x_1,x_2\in\mathbb{F}_q^*} \chi_1(x_1 + x_2 + a x_1^{-1} x_2^{-1}) \Big\} + q^7 \Big\{ \sum_{a\in\mathbb{F}_q} \chi_1(-a\beta) - 1 \Big\} \\
&= q^4 \Big\{ \sum_{x_1,x_2\in\mathbb{F}_q^*} \chi_1(x_1 + x_2) \sum_{a\in\mathbb{F}_q^*} \chi_1(a(x_1^{-1}x_2^{-1} - \beta)) \Big\} + q^7 \sum_{a\in\mathbb{F}_q} \chi_1(-a\beta) - q^7 \\
&= q^4 \Big\{ \sum_{x_1,x_2\in\mathbb{F}_q^*} \chi_1(x_1 + x_2) \sum_{a\in\mathbb{F}_q} \chi_1(a(x_1^{-1}x_2^{-1} - \beta)) - \sum_{x_1,x_2\in\mathbb{F}_q^*} \chi_1(x_1 + x_2) \Big\} \\
&\quad + q^7 \sum_{a\in\mathbb{F}_q} \chi_1(-a\beta) - q^7 \\
&= q^4 \Big\{ q \sum_{\substack{x_1,x_2\in\mathbb{F}_q^* \\ x_1^{-1}x_2^{-1}=\beta}} \chi_1(x_1 + x_2) + (-1)^3 \Big\} + q^7 \sum_{a\in\mathbb{F}_q} \chi_1(-a\beta) - q^7 \\
&= \begin{cases} q^8 - q^7 - q^4 & \text{if } \beta = 0, \\ q^5 K(\chi_1; \beta^{-1}) - q^7 - q^4 & \text{if } \beta \neq 0. \end{cases}
\end{aligned}$$

□

PROPOSITION 2.9. *Let* $n_\beta = |\{g \in Sp(4, q) \mid \mathrm{Tr}(g) = \beta\}|$, *for each* $\beta \in \mathbb{F}_q$. *Then*

$$n_\beta = \begin{cases} q^9 - q^6 - q^5 & \text{if } \beta = 0, \\ q^4\{K(\chi_1; \beta^{-1}) + q^5 - q^3 - q^2 - q\} & \text{if } \beta \neq 0. \end{cases}$$

PROOF.

$$\begin{aligned}
q n_\beta &= \sum_{g\in Sp(4,q)} \sum_{a\in\mathbb{F}_q} \chi_a(\mathrm{Tr}\, g) \overline{\chi}_a(\beta) \\
&= \sum_{a\in\mathbb{F}_q} \overline{\chi}_a(\beta) \sum_{g\in Sp(4,q)} \chi_a(\mathrm{Tr}\, g) \\
&= |Sp(4, q)| + \sum_{a\in\mathbb{F}_q^*} \overline{\chi}_a(\beta) \sum_{g\in Sp(4,q)} \chi_a(\mathrm{Tr}\, g).
\end{aligned}$$

Our results now follow from (1.1) and (2.5). □

The following corollary is immediate from the above proposition.

COROLLARY 2.10. $\mathrm{Tr} : Sp(4, q) \to \mathbb{F}_q$ *is surjective.*

https://doi.org/10.1017/S0004972708001366 Published online by Cambridge University Press

PROOF. From Proposition 2.9 and using the Weil bound $|K(\chi_1; a)| \le 2\sqrt{q}(a \in \mathbb{F}_q^*)$, we see that

$$n_\beta = |\{g \in Sp(4, q) \mid \mathrm{Tr}(g) = \beta\}| > 0 \quad \text{for all } \beta \in \mathbb{F}_q. \qquad \square$$

THEOREM 2.11. *$\Psi : \mathbb{F}_q \to C^\perp(Sp(4, q))$ with $\Psi(a) = c(a)$ is an $\mathbb{F}_2$-linear isomorphism.*

PROOF. It is $\mathbb{F}_2$-linear and surjective. Let a be in Ker Ψ. Then $tr(a\mathrm{Tr}(g)) = 0$, for all $g \in Sp(4, q)$. In view of Corollary 2.10, $tr(a\beta) = 0$, for all $\beta \in \mathbb{F}_q$. Since the trace map $tr : \mathbb{F}_q \to \mathbb{F}_2$ is surjective, $a = 0$. $\square$

PROPOSITION 2.12. *For $a \in \mathbb{F}_q^*$, the Hamming weight of the codeword*

$$c(a) = (tr(a\mathrm{Tr}(g_1)), \ldots, tr(a\mathrm{Tr}(g_N)))$$

is given by

$$w(c(a)) = \tfrac{1}{2}(N - q^4\{K(\chi_1; a)^2 + q^3 - q\}) \tag{2.6}$$
$$= \tfrac{1}{2}(N - q^4\{K_2(\chi_1; a) + q^3\}). \tag{2.7}$$

PROOF.

$$w(c(a)) = \frac{1}{2}\sum_{i=1}^{N}(1 - (-1)^{tr(a\mathrm{Tr}(g_i))})$$
$$= \frac{1}{2}\Big(N - \sum_{i=1}^{N} \chi_1(a\mathrm{Tr}(g_i))\Big). \qquad \square$$

Our results now follow from (1.1) and (2.2)–(2.3).

3. Proof of main results

THEOREM 3.1 (Pless Power Moment Identity [8]). *Let B be a q-ary [n,k] code, and let B_i (respectively $B_i^\perp$) denote the number of codewords of weight i in B (respectively in $B^\perp$). Then, for $h = 0, 1, \ldots,$*

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

where $S(h, t)$ denotes the Stirling number of the second kind defined by

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

https://doi.org/10.1017/S0004972708001366 Published online by Cambridge University Press

THEOREM 3.2 (Lachaud and Wolfman [6]). *Let $q = 2^r$, with $r \geq 2$. Then the range R of $K(\chi_1; a)$, as a varies over $\mathbb{F}_q^*$, is given by*

$$R = \{t \in \mathbb{Z} \mid |t| < 2\sqrt{q},\ t \equiv -1 (\text{mod } 4)\}.$$

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.

Let $u = (u_1, \ldots, u_N) \in \mathbb{F}_q^N$, with ν_β 1s in the coordinate places where $\mathrm{Tr}(g_j) = \beta$, for each $\beta \in \mathbb{F}_q$. Then we see from the definition of the code $C = C(Sp(4, q))$ that u is a codeword with weight i if and only if $\sum_{\beta \in \mathbb{F}_q} \nu_\beta = i$ and $\sum_{\beta \in \mathbb{F}_q} \nu_\beta \beta = 0$ (an identity in $\mathbb{F}_q$). As there are $\prod_{\beta \in \mathbb{F}_q} \binom{n_\beta}{\nu_\beta}$ many such codewords with weight i, we obtain the following theorem.

THEOREM 3.3. *Let $\{C_i\}_{i=0}^N$ be the weight distribution of the code $C = C(Sp(4, q))$. Then, for $0 \leq i \leq N$,*

$$C_i = \sum \binom{q^9 - q^6 - q^5}{\nu_0} \prod_{\beta \in \mathbb{F}_q^*} \binom{n_\beta}{\nu_\beta}, \tag{3.1}$$

where $n_\beta = q^4\{K(\chi_1; \beta^{-1}) + q^5 - q^3 - q^2 - q\}$ and the sum runs over all the sets of nonnegative integers $\{\nu_\beta\}_{\beta \in \mathbb{F}_q}$ satisfying $\sum_{\beta \in \mathbb{F}_q} \nu_\beta = i$ and $\sum_{\beta \in \mathbb{F}_q} \nu_\beta \beta = 0$.

COROLLARY 3.4. *Assume that $r \geq 2$, and that $\{C_i\}_{i=0}^N$ is the weight distribution of the code $C = C(Sp(4, q))$. Then, for $0 \leq i \leq N$,*

$$C_i = \sum \binom{m_0}{\nu_0} \prod_{\substack{|t| < 2\sqrt{q} \\ \text{with } t \equiv -1 (\text{mod } 4)}} \prod_{K(\chi_1; \beta^{-1}) = t} \binom{m_t}{\nu_\beta},$$

where

$$m_0 = n_0 = q^9 - q^6 - q^5,$$

and

$$m_t = q^4(q^5 - q^3 - q^2 - q + t),$$

for all $t \in \mathbb{Z}$ satisfying $|t| < 2\sqrt{q}$, and $t \equiv -1 (\text{mod } 4)$.

We are now ready to prove Theorem 1.1, which is the main result of this paper.

PROOF OF THEOREM 1.1. We apply the Pless power moment identity with $B = C^\perp(Sp(4, q))$. Then, with $\{C_i^\perp\}_{i=0}^N$ the weight distribution of $C^\perp(Sp(4, q))$, we have

$$\sum_{i=0}^{N} i^h C_i^\perp = \sum_{i=0}^{\min\{N,h\}} (-1)^i C_i \sum_{t=i}^{h} t! S(h, t) 2^{r-t} \binom{N - i}{N - t}. \tag{3.2}$$

https://doi.org/10.1017/S0004972708001366 Published online by Cambridge University Press

The left-hand side of (3.2) is given by

$$\begin{aligned}\sum_{i=0}^{N} i^h C_i^{\perp} &= \sum_{a\in\mathbb{F}_q^*} w(c(a))^h \quad \text{(By Theorem 2.11)}\\ &= \frac{1}{2^h}\sum_{a\in\mathbb{F}_q^*}(N-q^4\{K(\chi_1;a)^2+q^3-q\})^h \quad \text{(By (9))}\\ &= \frac{1}{2^h}\sum_{i=0}^{h}(-1)^i\binom{h}{i}(N-q^7+q^5)^{h-i}q^{4i}MK^{2i}\\ &= \frac{1}{2^h}(-1)^h q^{4h}MK^{2h}+\frac{1}{2^h}\sum_{i=0}^{h-1}(-1)^i\binom{h}{i}(N-q^7+q^5)^{h-i}q^{4i}MK^{2i}.\end{aligned}$$

On the other hand, the right-hand side of (3.2) is given by

$$\frac{q}{2^h}\sum_{i=0}^{\min\{N,h\}}(-1)^i C_i \sum_{t=i}^{h} t!S(h,t)2^{h-t}\binom{N-i}{N-t}.$$

Here the frequencies C_i of codewords with weight i in $C = C(Sp(4,q))$ are given by (3.1).

Now, Corollary 1.2 follows from (2.7).

References

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

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

[3] D. S. Kim, 'Gauss sums for symplectic groups over a finite field', *J. Monatsh. Math.* **126** (1998), 55–71.

[4] ———, 'Codes associated with special linear groups and power moments of multi-dimensional Kloosterman sums', submitted.

[5] 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.

[6] 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.

[7] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd edn, Encyclopedia of Mathematics and its Applications, 20 (Cambridge University Press, Cambridge, UK, 1997).

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

[9] 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**(2) (2007), 843–847.

[10] ———, 'Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm', *Acta Arith.* **132**(4) (2008), 329–350.

[11] M. Moisio and K. Ranto, 'Kloosterman sum identities and low-weight codewords in a cyclic code with two zeros', *Finite Fields Appl.* **13** (2007), 922–935.

[12] 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.

https://doi.org/10.1017/S0004972708001366 Published online by Cambridge University Press

JI HYUN KIM, Department of Mathematics, Sogang University, Seoul 121–742, South Korea
e-mail: mip97@hanmail.net

https://doi.org/10.1017/S0004972708001366 Published online by Cambridge University Press