Volume 114 Issue 2 February 2007 ISSN 0097-3165

Journal of Combinatorial Theory

Series A

Available online at www.sciencedirect.com
ScienceDirect
ELSEVIER
Journal of Combinatorial Theory, Series A 114 (2007) 322–338
Journal of Combinatorial Theory Series A
www.elsevier.com/locate/jcta

The divisibility modulo 24 of Kloosterman sums on $GF(2^m)$, m odd ☆

Pascale Charpin [a], Tor Helleseth [b], Victor Zinoviev [c]

[a] *INRIA, Domaine de Voluceau-Rocquencourt, BP 105-78153, Le Chesnay, France*
[b] *Department of Informatics, University of Bergen, N-5020 Bergen, Norway*
[c] *Institute for Problems of Information Transmission, Russian Academy of Sciences, Bol'shoi Karetnyi per. 19, GSP-4, Moscow 101447, Russia*

Received 18 October 2005

Available online 12 July 2006

Communicated by Vera Pless

Abstract

In a previous paper, we studied the cosets of weight 4 of binary extended 3-error-correcting BCH codes of length 2^m (where m is odd). We expressed the number of codewords of weight 4 in such cosets in terms of exponential sums of three types, including the Kloosterman sums $\mathcal{K}(a)$, $a \in \mathbf{F}^*$. In this paper, we derive some congruences which link Kloosterman sums and cubic sums. This allows us to study the divisibility of Kloosterman sums modulo 24. More precisely, if we know the traces of a and of $a^{1/3}$, we are able to evaluate $\mathcal{K}(a)$ modulo 24 and to compute the number of those a giving the same value of $\mathcal{K}(a)$ modulo 24.

Keywords: 3-Error-correcting BCH code; Coset; Melas code; Irreducible code; Divisibility; Kloosterman sum; Cubic sum; Inverse-cubic sum; Quadratic mapping; Jacobi symbol

1. Introduction

This paper is a natural continuation of our previous papers [4,5,9]. Here we exploit the connection between binary primitive (in narrow sense) extended BCH codes of length 2^m (m odd) with minimal distance 8 and Kloosterman sums over finite fields of order 2^m. In [4], the coset

☆ This work was supported by INRIA-Rocquencourt, by the Norwegian Research Council and also by the Russian fund of fundamental researches (project 03-01-00098).

E-mail address: pascale.charpin@inria.fr (P. Charpin).

0097-3165/$ – see front matter © 2006 Elsevier Inc. All rights reserved.
doi:10.1016/j.jcta.2006.06.002

weight distributions of such BCH codes was described. It was proved that all these distributions are known as soon as they are known for cosets of weight 4. We indicated, for $m = 7$, the surprising distribution of the number of leaders in each coset of weight 4. In [9], the coset weight distributions of the Z_4-linear Goethals codes are considered. For the cosets of weight 4, the number of codewords of weight 4 was expressed in terms of Kloosterman sums. Using this last approach, and considering again the BCH codes, we found in [5] the exact expression of the number of codewords of weight 4 (in cosets of weight 4) in terms of exponential sums of three different types including Kloosterman sums. In this paper, we exploit the deep connection between cubic and Kloosterman sums which appeared in [5].

The paper is organized as follows. After some preliminaries, we present in Section 3 our main expression established in [5] as a congruence (Theorem 1 and (8)). We derive some properties, notably on the divisibility of the inverse-cubic sums (Lemma 5).

By Theorem 2 we state the key congruences which will allow us to compute the divisibility of Kloosterman sums modulo 24. All the results are given by Theorem 3 providing six different cases which depend each on the form of m. In Section 5, we recall the connection between Kloosterman sums and the $[2^m + 1, 2m]$ irreducible code and explain the consequences of our results on the weight distribution of this code.

Finally, in the last section, we compute for each case provided by Theorem 3 the number of times this case occurs (Table 2). We then contribute to the knowledge of the spectrum of Kloosterman sums which is, equivalently, the knowledge of the weight distribution of Melas codes or of the $[2^m + 1, 2m]$ irreducible codes. A part of our results in this paper was presented in [6].

2. Preliminaries

In this paper, the mappings are generally defined on $\mathbf{F}_{2^m}$, the finite field of order 2^m, with m odd and $m \geqslant 5$.[1] For any such mapping f, we will consider the Boolean function $x \mapsto \mathrm{Tr}(f(x))$ where Tr is the trace-function from $\mathbf{F}_{2^m}$ to $\mathbf{F}_2$. For simplicity, we will use this notation:

$$e\big(f(x)\big) = (-1)^{\mathrm{Tr}(f(x))}.$$

Also $\#T$ will denote the cardinality of any set T.

2.1. Exponential sums

Now, we need to define several exponential sums on $\mathbf{F}_{2^m}$.

Definition 1. The Kloosterman sums are:

$$\mathcal{K}(a) = \sum_{x \in \mathbf{F}_{2^m}} e\left(\frac{1}{x} + ax\right), \quad a \in \mathbf{F}_{2^m}.$$

The cubic sums are:

$$C(a,b) = \sum_{x \in \mathbf{F}_{2^m}} e\big(ax^3 + bx\big), \quad a \in \mathbf{F}_{2^m}^*,\ b \in \mathbf{F}_{2^m}.$$

[1] Note that for $m = 3$ the Kloosterman sums are cubic sums and the 3-error-correcting BCH codes do not exist.

The *inverse-cubic* sums are:

$$G(a,b)=\sum_{x\in\mathbf{F}_{2^m}} e\left(\frac{a}{x^3}+bx\right),\quad a\in\mathbf{F}_{2^m}^*,\ b\in\mathbf{F}_{2^m}.$$

For simplicity, $G(a,a)$ will be denoted by $G(a)$ and $C(1,b)$ by $C(b)$.

The Kloosterman sums and the inverse-cubic sums are generally defined on $\mathbf{F}_{2^m}^*$, the multiplicative group of $\mathbf{F}_{2^m}$. We extend them to 0, assuming that $e(x^{-1})=e(x^{-3})=1$ for $x=0$. Actually, we consider the Boolean functions on $\mathbf{F}_{2^m}$:

$$\mathrm{Tr}\left(\frac{1}{x}\right)=\mathrm{Tr}\big(x^{2^{m-1}-1}\big)\quad\text{and}\quad\mathrm{Tr}\left(\frac{1}{x^3}\right)=\mathrm{Tr}\big(x^{2^{m-2}-1}\big).$$

Note that, since the mappings $x\mapsto x^{2^{m-1}-1}$, $x\mapsto x^{2^{m-2}-1}$ and $x\mapsto x^3$ are permutations on $\mathbf{F}_{2^m}$ when m is odd, we have (for any a):

$$\mathcal{K}(0)=G(a,0)=C(a,0)=0.$$

The next lemma is directly obtained from the result of Lachaud and Wolfmann [11, Theorem 3.4] which is suitable for any m (even or odd). We only replace the sum on $\mathbf{F}_{2^m}^*$, denoted $K(a)$ in [11], by $\mathcal{K}(a)=K(a)+1$.

Lemma 1. *The set $\mathcal{K}(a), a\in\mathbf{F}_{2^m}$, is the set of all the integers $s\equiv 0 \pmod 4$ with $s-1$ in the range $[-2^{(m+2)/2}, 2^{(m+2)/2}]$.*

Moreover, the following result is due to Helleseth and Zinoviev [9].

Lemma 2. *For any m (odd or even)*

$$\mathcal{K}(a)\equiv\begin{cases}4 \pmod 8 & \text{if } \mathrm{Tr}(a)=1,\\ 0 \pmod 8 & \text{if } \mathrm{Tr}(a)=0.\end{cases}$$

2.2. *Quadratic sums*

Let $i>0$ and $a\in\mathbf{F}_{2^m}$. The spectrum of quadratic sums on $\mathbf{F}_{2^m}$ of the form

$$S(i,a,b)=\sum_{x\in\mathbf{F}_{2^m}} e\big(ax^{2^i+1}+bx\big),\quad b\in\mathbf{F}_{2^m} \tag{1}$$

is well-known. It is obtained by computing the *rank* of the symplectic form of the Boolean function $x\mapsto\mathrm{Tr}(ax^{2^i+1})$. The values $S(i,a,b)$, when b runs through $\mathbf{F}_{2^m}$, and the number of times they occur, only depend on this rank, usually denoted by $r=2h$. That is:

$$\begin{aligned}&0 \text{ occurs } 2^m-2^{2h} \text{ times};\\ &2^{m-h} \text{ occurs } 2^m+2^{h-1} \text{ times};\\ &-2^{m-h} \text{ occurs } 2^m-2^{h-1} \text{ times}.\end{aligned} \tag{2}$$

These properties are explained in [12, Chapter 15] and [10,13].

In this paper, m is odd. We mainly need the sums $S(1,1,b)$, $b\in\mathbf{F}_{2^m}$ (the cubic sums), and the sum $S(3,1,1)$ (see Proposition 5). For clarity, the spectrum of the cubic sum is recalled in

Table 1
The spectrum of $C(b)$ (Definition 1)

Value	Number it occurs
0	2^{m-1}
$2^{(m+1)/2}$	$2^{m-2}+2^{(m-3)/2}$
$-2^{(m+1)/2}$	$2^{m-2}-2^{(m-3)/2}$

Table 1. It corresponds to the rank $m-1$, i.e., $h=(m-1)/2$. When $i=3$ in (1), and for odd m, the corresponding rank is $r=m-3$ if 3 divides m and $r=m-1$ otherwise (see [12, Fig. 15.2]).

On the other hand, it is generally difficult to know the sign of $S(i,a,b)$ for any fixed (i,a) and for a given b. For $i=1$ (and for odd m) this was specified by Carlitz in [3] by means of the Jacobi symbol $(\frac{2}{m})$ (also called the quadratic character). Recall that the Jacobi symbol is a generalization of the Legendre symbol which was introduced for any odd prime p:

$$\left(\frac{2}{p}\right)=\begin{cases}1, & \text{if 2 is a square modulo } p,\\ -1, & \text{otherwise.}\end{cases} \tag{3}$$

We will need the exact expression of the Jacobi symbol.

Proposition 1. *Let m be odd. Set $m=m_1\cdots m_s$, where $s\geqslant 1$ and each m_i is an odd prime. Then*

$$\left(\frac{2}{m}\right)=\left(\frac{2}{m_1}\right)\cdots\left(\frac{2}{m_s}\right).$$

Moreover,

$$\left(\frac{2}{m}\right)=(-1)^{(m^2-1)/8}=\begin{cases}1 & \textit{for } m\equiv\pm 1 \pmod 8,\\ -1 & \textit{for } m\equiv\pm 3 \pmod 8.\end{cases} \tag{4}$$

In the next lemma, we give a slightly different version of the result of Carlitz [3, Theorem 2].

Lemma 3. *Let m be odd. Recall that $C(b)=\sum_{x\in\mathbf{F}_{2^m}}e(x^3+bx)$, $b\in\mathbf{F}_{2^m}$ (Definition 1). Then we have:*

(i) $C(1)=(\frac{2}{m})2^{(m+1)/2}$, *where $(\frac{2}{m})$ is the Jacobi symbol*;
(ii) *if* $\mathrm{Tr}(b)=1$ (*with* $b\neq 1$), *then*

$$C(b)=e\big(\beta^3\big)\left(\frac{2}{m}\right)2^{(m+1)/2},$$

where β is unique in $\mathbf{F}_{2^m}$ satisfying $b=\beta^4+\beta+1$ with $\mathrm{Tr}(\beta)=0$;
(iii) *if* $\mathrm{Tr}(b)=0$, *then $C(b)=0$.*

Proof. Comparing to the theorem of Carlitz, only (ii) is slightly modified. In [3] the expression of $C(b)$ is

$$C(b)=e\big(\beta^3+\beta\big)\left(\frac{2}{m}\right)2^{(m+1)/2},$$

where $b=\beta^4+\beta+1$ for some β.

The mapping $g : x \mapsto x^4 + x + 1$ is two-to-one on $\mathbf{F}_{2^m}$ and $g(x) = g(x+1)$. More precisely, for any b such that $\mathrm{Tr}(b) = 1$ there are exactly two elements β and $\beta + 1$ such that $b = \beta^4 + \beta + 1$. But

$$\mathrm{Tr}\big((\beta+1)^3 + \beta + 1\big) = \mathrm{Tr}\big(\beta^3 + \beta^2\big) = \mathrm{Tr}\big(\beta^3 + \beta\big).$$

Thus we can define β as the unique element in the pair $(\beta, \beta+1)$ which satisfies $\mathrm{Tr}(\beta) = 0$. Moreover, $e(\beta^3 + \beta) = e(\beta^3)$ completing the proof of (ii). □

In Section 6, we will need specific results on quadratic sums. It is first the next formula:

$$C(1) = 2 \sum_{x \in \mathbf{F}_{2^m},\, \mathrm{Tr}(x)=0} e\big(x^3\big) = -2 \sum_{x \in \mathbf{F}_{2^m},\, \mathrm{Tr}(x)=1} e\big(x^3\big). \tag{5}$$

This formula holds because

$$\sum_{x \in \mathbf{F}_{2^m}} e\big(x^3 + x\big) = \sum_{x \in \mathbf{F}_{2^m},\, \mathrm{Tr}(x)=0} e\big(x^3\big) - \sum_{x \in \mathbf{F}_{2^m},\, \mathrm{Tr}(x)=1} e\big(x^3\big).$$

But $C(0) = 0$ meaning that $\sum_{\mathrm{Tr}(x)=0} e(x^3) = -\sum_{\mathrm{Tr}(x)=1} e(x^3)$.

We will need a basic property of quadratic functions. A proof of the next lemma can be found in [2, Proposition II-5]. First recall that any Boolean function f on $\mathbf{F}_{2^m}$ is said to be *balanced if the number of those x such that $f(x) = 1$, i.e., the weight of f is equal to* 2^{m-1}. In this case, we have obviously

$$\sum_{x \in \mathbf{F}_{2^m}} (-1)^{f(x)} = 0.$$

Lemma 4. *Let f be any quadratic Boolean function f on $\mathbf{F}_{2^m}$. Then f is balanced if and only if there is $u \in \mathbf{F}_{2^m}^*$ such that*

$$f(x) + f(x+u) = 1, \quad \forall x.$$

In the next example, we point out the balanceness of a special class of quadratic Boolean functions.

Example 1. Set $f(x) = \sum_{i \in I} \mathrm{Tr}(x^{2^i+1})$ where $I \subset \{0, 1, \ldots, m-1\}$, m odd. Then we have for any $x \in F$:

$$\begin{aligned} f(x) + f(x+1) &= \sum_{i \in I} \mathrm{Tr}\big(x^{2^i} + x + 1\big) = \sum_{i \in I} \mathrm{Tr}(1) \\ &\equiv \#I \pmod 2. \end{aligned}$$

Thus, *when m is odd, such f is balanced if the cardinality of I is odd.*

3. Cosets of the 3-error-correcting extended BCH code

Let us denote by B the binary BCH code of length $n = 2^m$, m odd and $m \geqslant 5$, with minimal distance 8. Finding the number of words in a coset of weight 4 of B needs to solve the following system of equations over $\mathbf{F}_{2^m}$:

$$\left.\begin{aligned} x + y + z + u &= a, \\ x^3 + y^3 + z^3 + u^3 &= b, \\ x^5 + y^5 + z^5 + u^5 &= c. \end{aligned}\right\} \tag{6}$$

Here x, y, z and u are pairwise distinct elements of $\mathbf{F}_{2^m}$ and $a, b, c \in \mathbf{F}_{2^m}$ are fixed. Let $\mu(a, b, c)$ be the number of different such 4-tuples (x, y, z, u) which are solutions to the system (6). Assume that $a \neq 0$. Then there are $\epsilon \in \{0, 1\}$ and $\eta \in \mathbf{F}_{2^m}$ such that $\mu(a, b, c) = \mu(1, \epsilon, \eta)$. To be more precise

$$\epsilon = \mathrm{Tr}\left(\frac{b}{a^3}\right) \quad \text{and} \quad \eta = \frac{c}{a^5} + \frac{b^2}{a^6} + \frac{b}{a^3}$$

are uniquely defined, as explained in [5]. The condition $a \neq 0$ means that the corresponding coset is contained in the Reed–Muller code of order $m - 1$ and not contained in the Reed–Muller code of order $m - 2$, i.e., (x, y, z, u) is not a flat. The reader can refer to [4] for a complete explanation of the types of cosets of 3-error-correcting extended BCH codes. In [5] we established that $\mu(1, \epsilon, \eta)$ can be expressed in terms of exponential sums.

Theorem 1. *Let $\mu(1, \epsilon, \eta)$, $\epsilon \in \{0, 1\}$ and $\eta \in \mathbf{F}_{2^m}$, as above defined. Then $\mu(1, \epsilon, \eta)$ is even and can be expressed as follows: for $\eta \neq 1$*

$$\begin{aligned} 24 \times \mu(1, \epsilon, \eta) = {} & 2^m - 8\big(1 + (-1)^{\epsilon+1}\big) + 3 \cdot G(\eta + 1) \\ & + (-1)^{\epsilon+1} \cdot 2 \cdot \big(\mathcal{K}(\eta + 1) + C\big((\eta + 1)^{1/3}\big)\big). \end{aligned} \tag{7}$$

Furthermore, when $\eta = 1$ then $\mu(1, \epsilon, 1) = 0$.

Remark 1. The expression of $\mu(1, \epsilon, \eta)$ in [5] is of the form

$$2^m - 5 + 3 \cdot G' + (-1)^{\epsilon+1} \cdot 2 \cdot \big(K' + C\big((\eta + 1)^{1/3}\big) - 3\big),$$

where $G' = G(\eta + 1) - 1$ and $K' = \mathcal{K}(\eta + 1) - 1$ (these sums were computed on $\mathbf{F}^*_{2^m}$, not on $\mathbf{F}_{2^m}$).

From now on $\mu(\epsilon, \eta) = \mu(1, \epsilon, \eta)$ and $G(a, a)$ is denoted $G(a)$, for simplicity. There are several consequences of the previous theorem. We deduce easily that for $m \geqslant 9$ there are solutions of (6) except for the (a, b, c) corresponding to $(1, \epsilon, 1)$. This leads to the determination of the number of cosets of weight 4, as we will explain in a forthcoming paper [7].

Corollary 1. *When $m \geqslant 9$ then $\mu(\epsilon, \eta) > 0$ for any $\epsilon \in \{0, 1\}$ and for any $\eta \neq 1$. Consequently, for any such (ϵ, η) and for $m \geqslant 9$:*

$$\begin{aligned} & 2^m - 8\big(1 + (-1)^{\epsilon+1}\big) + 3 \cdot G(\eta + 1) \\ & \quad + (-1)^{\epsilon+1} \cdot 2 \cdot \big(\mathcal{K}(\eta + 1) + C\big((\eta + 1)^{1/3}\big)\big) \equiv 0 \pmod{48}. \end{aligned} \tag{8}$$

Proof. From Lemmas 1 and 3, we have:

$$C\big((\eta + 1)^{1/3}\big) \in \big\{0, \pm 2^{(m+1)/2}\big\} \quad \text{and} \quad \big|\mathcal{K}(\eta + 1)\big| < 2^{(m/2)+1} + 1,$$

where $|\lambda|$ denotes the absolute value of λ. Moreover, we proved in [5] that $|G(\eta + 1)| < 2^{(m/2)+2} + 1$. We consider the equality (7) and we have to prove that the term on the right is strictly positive. We consider

$$A_m = 3 \cdot G(\eta + 1) + (-1)^{\epsilon+1} \cdot 2 \cdot \big(\mathcal{K}(\eta + 1) + C\big((\eta + 1)^{1/3}\big)\big).$$

From the previous bounds we get:

$$|A_m| < 3 \cdot 2^{(m/2)+2} + 2\big(2^{(m/2)+1} + 2^{(m+1)/2}\big) + 5$$

which implies

$$|A_m| < 4 \cdot 2^{(m/2)+2} + 2^{(m+3)/2} + 5.$$

We want to prove that $2^m - 8(1 + (-1)^{\epsilon+1}) + A_m > 0$. Clearly this is true as soon as $(m/2) + 4 < m$, that is $m + 8 < 2m$ which is $8 < m$.

Thus, we know that, for $m \geqslant 9$, $\mu(\epsilon, \eta)$ is a nonzero positive even number. In accordance with (7) we directly obtain (8). □

Remark 2. Let B be the 3-error correcting extended BCH code. When $m = 5$, B is in fact the self-dual Reed–Muller code. The weight distribution of cosets of B is known [1]. When $m = 7$, the weight distribution of cosets of B was computed in [4]. Note that for $m < 9$ the values $\mathcal{K}(a)$ are easily computed (see Tables 4 and 5).

Moreover, we are able to deduce a property on the divisibility of inverse-cubic sums $G(a)$. Note that it is suitable for odd m only. Recall that $G(a) = \sum_{x \in \mathbf{F}_{2^m}} e(a/x^3 + ax)$.

Lemma 5. *For any odd m, $m \geqslant 5$,*

$$G(a) \equiv \begin{cases} 8 \pmod{16}, & \textit{if } \mathrm{Tr}(a) = 1, \\ 0 \pmod{16}, & \textit{if } \mathrm{Tr}(a) = 0. \end{cases}$$

Proof. We use (7) with $a = \eta + 1$, $a \neq 0$. Note that $G(0) = 2^m$ is a trivial case. The cubic sum $C(a^{1/3})$ is congruent to 0 modulo $2^{(m+1)/2}$. Thus $2C(a^{1/3})$ is congruent to 0 modulo 16 as soon as $(m+3)/2 \geqslant 4$ which is $m \geqslant 5$. Since $2^m - 8(1 + (-1)^{\epsilon+1})$ is 0 modulo 16 for any $\epsilon \in \{0, 1\}$, we then deduce from (7):

$$\pm 2 \cdot \mathcal{K}(a) + 3 \cdot G(a) \equiv 0 \pmod{16}.$$

Now we apply Lemma 2. If $\mathrm{Tr}(a) = 1$ then $2\mathcal{K}(a) \equiv 8$ modulo 16 implying that $G(a) \equiv 8$ modulo 16 too. When $\mathrm{Tr}(a) = 0$, $2\mathcal{K}(a) \equiv 0$ modulo 16 and then $G(a) \equiv 0$ modulo 16. □

4. Divisibility of Kloosterman sums

The following relations between cubic and Kloosterman sums are deduced from (7) (with $a = \eta + 1$, $a \neq 0$), Lemmas 2 and 3. Recall that $m \geqslant 5$.

Theorem 2 *(The key congruences). For any a, $a \in \mathbf{F}_{2^m}^*$, we have: If* $\mathrm{Tr}(a) = 0$ *then*

$$C\big(a^{1/3}\big) + \mathcal{K}(a) \equiv 16 \pmod{24} \tag{9}$$

else

$$C\big(a^{1/3}\big) + \mathcal{K}(a) \equiv 4 \pmod{24}. \tag{10}$$

Proof. First note that for any integer r, $r \geqslant 1$, we have:

$$2^r \equiv (-1)^r \pmod{3}.$$

Thus, since m is odd, we deduce from (7):

$$2 + \big(1 + (-1)^{\epsilon+1}\big) + (-1)^{\epsilon+1} \cdot 2 \cdot \big(\mathcal{K}(a) + C\big(a^{1/3}\big)\big) \equiv 0 \pmod{3}.$$

This gives the same congruence for $\epsilon = 0$ and $\epsilon = 1$:

$$\mathcal{K}(a) + C\big(a^{1/3}\big) \equiv 1 \pmod 3. \tag{11}$$

Now $C(a^{1/3}) \equiv 0$ modulo 8 as soon as $m \geqslant 5$ (Lemma 3). Hence

$$\mathcal{K}(a) + C\big(a^{1/3}\big) \equiv \mathcal{K}(a) \pmod 8.$$

We apply Lemma 2. Set $L(a) = \mathcal{K}(a) + C(a^{1/3})$. If $\mathrm{Tr}(a) = 0$ then $L(a) = 8R$, for some integer R, which leads to $L(a) \equiv 2R$ modulo 3. According to (11) we get $R \equiv 2$ modulo 3. Consequently $L(a) \equiv 16$ modulo 24.

Similarly, if $\mathrm{Tr}(a) = 1$ then $L(a) = 8R + 4$ leads to $L(a) \equiv 2R + 1$ modulo 3. Then we get $R \equiv 0$ modulo 3 which implies $L(a) \equiv 4$ modulo 24, completing the proof. □

In accordance with the previous theorem, it appears that the divisibility of the sums $\mathcal{K}(a)$ modulo 24 is strongly related with those of the cubic sums. This fact will be specified by proving the next three corollaries.

Corollary 2. *Assume that* $\mathrm{Tr}(a^{1/3}) = 0$, $a \in \mathbf{F}_{2^m}^*$. *Then*

$$\mathcal{K}(a) \equiv \begin{cases} 16 \pmod{24} & \textit{if } \mathrm{Tr}(a) = 0, \\ 4 \pmod{24} & \textit{if } \mathrm{Tr}(a) = 1. \end{cases}$$

Proof. Recall that $C(a^{1/3}) = 0$ if and only if $\mathrm{Tr}(a^{1/3}) = 0$. Thus, one simply rewrites (9) and (10) with $C(a^{1/3}) = 0$. □

When $C(b) \neq 0$, for some $b \in \mathbf{F}_{2^m}$, then $C(b) = \pm 2^\rho$ with $\rho = (m+1)/2$. Since $2^\rho = 8(3-1)^{\rho-3}$, we get

$$2^\rho \equiv \begin{cases} 16 \pmod{24} & \text{if } \rho \text{ is even}, \\ 8 \pmod{24} & \text{if } \rho \text{ is odd}. \end{cases} \tag{12}$$

Set $m = 4h + \tau$ with $\tau \in \{1, 3\}$. Since $2\rho = 4h + \tau + 1$, we have clearly

$$\rho \text{ is odd} \quad \Leftrightarrow \quad m = 4h + 1 \quad \text{and} \quad \rho \text{ is even} \quad \Leftrightarrow \quad m = 4h + 3. \tag{13}$$

The next proposition comes directly from (12) and (13).

Proposition 2. *Let* $b \in \mathbf{F}_{2^m}$ *such that* $C(b) \neq 0$. *Thus* $C(b) = \pm 2^{(m+1)/2}$ *with*:

$$2^{(m+1)/2} \equiv \begin{cases} 16 \pmod{24} & \textit{if } m = 4h + 3, \\ 8 \pmod{24} & \textit{if } m = 4h + 1 \end{cases}$$

and

$$-2^{(m+1)/2} \equiv \begin{cases} 8 \pmod{24} & \textit{if } m = 4h + 3, \\ 16 \pmod{24} & \textit{if } m = 4h + 1. \end{cases}$$

Now we are able to treat (9) and (10) when $C(a^{1/3}) \neq 0$. Among the next corollaries, we will prove the first only. The proof of the other is symmetrically obtained.

Corollary 3. *Assume that* $a \in \mathbf{F}_{2^m}^*$ *is such that* $\mathrm{Tr}(a^{1/3}) \neq 0$ *with* $C(a^{1/3}) = 2^{(m+1)/2}$. *Then*

$$\mathrm{Tr}(a) = 0 \quad \Rightarrow \quad \mathcal{K}(a) \equiv \begin{cases} 0 \pmod{24} & \textit{if } m = 4h + 3, \\ 8 \pmod{24} & \textit{if } m = 4h + 1 \end{cases}$$

and

$$\mathrm{Tr}(a)=1 \quad\Rightarrow\quad \mathcal{K}(a)\equiv\begin{cases}12 \pmod{24} & \textit{if } m=4h+3,\\ 20 \pmod{24} & \textit{if } m=4h+1.\end{cases}$$

Proof. If $\mathrm{Tr}(a)=0$ then (9) is satisfied. According to Proposition 2, we get $16+\mathcal{K}(a)\equiv 16$ when $m=4h+3$ and $8+\mathcal{K}(a)\equiv 16$ when $m=4h+1$. If $\mathrm{Tr}(a)=1$ then (10) is satisfied. Thus we get respectively $16+\mathcal{K}(a)\equiv 4$ and $8+\mathcal{K}(a)\equiv 4$, completing the proof. □

Corollary 4. *Assume that $a\in\mathbf{F}_{2^m}^*$ is such that $\mathrm{Tr}(a^{1/3})\neq 0$ with $C(a^{1/3})=-2^{(m+1)/2}$. Then*

$$\mathrm{Tr}(a)=0 \quad\Rightarrow\quad \mathcal{K}(a)\equiv\begin{cases}8 \pmod{24} & \textit{if } m=4h+3,\\ 0 \pmod{24} & \textit{if } m=4h+1\end{cases}$$

and

$$\mathrm{Tr}(a)=1 \quad\Rightarrow\quad \mathcal{K}(a)\equiv\begin{cases}20 \pmod{24} & \textit{if } m=4h+3,\\ 12 \pmod{24} & \textit{if } m=4h+1.\end{cases}$$

Using the terminology of Lemma 3, we summarize our results as follows.

Theorem 3. *Let a be any nonzero element of $\mathbf{F}_{2^m}$, where m is odd and $m\geqslant 5$. Then we have*

(1) *If* $\mathrm{Tr}(a^{1/3})=0$ *then*
   (a) *if* $\mathrm{Tr}(a)=0$ *then* $\mathcal{K}(a)\equiv 16 \pmod{24}$;
   (b) *if* $\mathrm{Tr}(a)=1$ *then* $\mathcal{K}(a)\equiv 4 \pmod{24}$.

(2) *When* $\mathrm{Tr}(a^{1/3})=1$ *then there is a unique β such that* $\mathrm{Tr}(\beta)=0$ *and* $a^{1/3}=\beta^4+\beta+1$. *Hence*
   (a) *if* $\mathrm{Tr}(a)=0$ *then*
      (i) *if* $m=4h+3$ *then*

$$\mathcal{K}(a)\equiv\begin{cases}0 \pmod{24} & \textit{if } e(\beta^3)(\frac{2}{m})=1,\\ 8 \pmod{24} & \textit{if } e(\beta^3)(\frac{2}{m})=-1;\end{cases}$$

      (ii) *if* $m=4h+1$ *then*

$$\mathcal{K}(a)\equiv\begin{cases}8 \pmod{24} & \textit{if } e(\beta^3)(\frac{2}{m})=1,\\ 0 \pmod{24} & \textit{if } e(\beta^3)(\frac{2}{m})=-1;\end{cases}$$

   (b) *if* $\mathrm{Tr}(a)=1$ *then*
      (i) *if* $m=4h+3$ *then*

$$\mathcal{K}(a)\equiv\begin{cases}12 \pmod{24} & \textit{if } e(\beta^3)(\frac{2}{m})=1,\\ 20 \pmod{24} & \textit{if } e(\beta^3)(\frac{2}{m})=-1;\end{cases}$$

      (ii) *if* $m=4h+1$ *then*

$$\mathcal{K}(a)\equiv\begin{cases}20 \pmod{24} & \textit{if } e(\beta^3)(\frac{2}{m})=1,\\ 12 \pmod{24} & \textit{if } e(\beta^3)(\frac{2}{m})=-1.\end{cases}$$

There is a surprising consequence of the previous theorem concerning the cases where $\mathcal{K}(a)$ is zero which can be expressed as follows.

Corollary 5. *If $a \in \mathbf{F}_{2^m}^*$ is such that $\mathcal{K}(a) = 0$ then* $\mathrm{Tr}(a) = 0$ *and* $\mathrm{Tr}(a^{1/3}) = 1$*. Moreover, in this case, $C(a^{1/3}) > 0$ for $m = 4h + 3$ and $C(a^{1/3}) < 0$ for $m = 4h + 1$.*

5. On the $[2^m + 1, 2m]$ irreducible binary code

In this section, we will denote by T_ℓ^k the trace function from $\mathbf{F}_{2^k}$ to $\mathbf{F}_{2^\ell}$, where ℓ divides k. Also, we denote by γ a primitive $(2^m + 1)$th root of unity in $\mathbf{F}_{2^{2m}}$ and by α a primitive root of $\mathbf{F}_{2^m}$. For any Boolean function f, the weight of f is the Hamming weight of the vector of its values.

Let us denote by C the binary irreducible $[2^m + 1, 2m]$ code. The codewords of C are precisely the vectors:

$$\mathbf{c}_u = \big\{T_1^{2m}(u), T_1^{2m}(u\gamma), \ldots, T_1^{2m}\big(u\gamma^{2^m}\big)\big\}, \quad u \in \mathbf{F}_{2^{2m}}. \tag{14}$$

Since $\gcd(2^m + 1, 2^m - 1) = 1$, each such u can be written $u = \alpha^i \gamma^j$. Thus $\mathbf{c}_u$ is a shift of $\mathbf{c}_{\alpha^i}$. Therefore, *for studying the weights of C we only have to consider the weights of those $\mathbf{c}_u$ with $u \in \mathbf{F}_{2^m}$.*

It was first proved by Dillon in [8] that the weights of the code C are exactly those of the dual of the Melas code, say $\mathcal{M}$. The code $\mathcal{M}$ is the cyclic binary $[2^m - 1, 2m]$ code whose nonzeros are α and α^{-1} only. Since the words of $\mathcal{M}$ are described by the functions $x \mapsto T_1^m(bx^{-1} + ax)$ on $\mathbf{F}_{2^m}^*$, the connection between the weights of $\mathcal{M}$ and the Kloosterman sums is clear. The reader can see [11] for more details and its generalization to any characteristic in [14]. We now present the result due to Dillon in our context. Note that the Hamming weight of any vector v is denoted $wt(v)$.

Theorem 4. [8] *Let $w_u = wt(\mathbf{c}_u)$, $u \in \mathbf{F}_{2^m}$, where $\mathbf{c}_u$ is defined by* (14)*. Let us denote by λ_u the weight of the function $x \mapsto T_1^m(x^{-1} + ux)$ defined on $\mathbf{F}_{2^m}$. Then $w_u = 2^m - \lambda_u$. Therefore the Kloosterman sums $\mathcal{K}(u)$ and the weights w_u are related by*:

$$\mathcal{K}(u) = -\big(2^m - 2w_u\big) = -\sum_{j=1}^{2^m} (-1)^{T_1^{2m}(u\gamma^j)}. \tag{15}$$

In other words, to compute the nonzero weights of C is exactly to compute the $\mathcal{K}(u)$, $u \in \mathbf{F}_{2^m}^*$.

Proof. Let us denote by $\mathcal{G}$ the cyclic subgroup of $\mathbf{F}_{2^{2m}}$ generated by γ. We have for any $u \in \mathbf{F}_{2^m}^*$ and for any $j \in [1, 2^m]$:

$$T_1^{2m}\big(u\gamma^j\big) = T_1^m T_m^{2m}\big(u\gamma^j\big) = T_1^m\big(u\big(\gamma^j + \gamma^{-j}\big)\big),$$

since $\gamma^{2^m+1} = 1$. Set $S = \{x \in \mathbf{F}_{2^m}^* \mid T_1^m(x^{-1}) = 1\}$. The function g from $\mathcal{G}$ to $\mathbf{F}_{2^m}$, defined by $g(y) = y + y^{-1}$, is zero for $y = 1$ only and takes exactly twice each value in S. This is because, for any b, the equation $y^2 + by + 1 = 0$ has two solutions in the quadratic extension of $\mathbf{F}_{2^m}$ if and only if $T_1^m(1/b) = 1$. Hence we have:

$$\begin{aligned} w_u &= \#\big\{j \in \big[1, 2^m\big] \bigm| T_1^m\big(u\big(\gamma^j + \gamma^{-j}\big)\big) = 1\big\} \\ &= 2\#\big\{x \in \mathbf{F}_{2^m}^* \bigm| T_1^m(ux) = 1 \text{ and } T_1^m\big(x^{-1}\big) = 1\big\}. \end{aligned}$$

Table 2
This table is explained at the end of Section 6

$m = 4h + 3$	$= 8s + 7$	$= 8s + 3$
N_1 [16]	$2^{m-2} + 2^{(m-3)/2} - 1$	$2^{m-2} - 2^{(m-3)/2} - 1$
N_2 [4]	$2^{m-2} - 2^{(m-3)/2}$	$2^{m-2} + 2^{(m-3)/2}$
N_3 [0]	$2^{m-3} - E/8$	$2^{m-3} + E/8 + 2^{(m-3)/2}$
N_4 [8]	$2^{m-3} + E/8 - 2^{(m-3)/2}$	$2^{m-3} - E/8$
N_5 [12]	$2^{m-3} + E/8 + 2^{(m-3)/2}$	$2^{m-3} - E/8$
N_6 [20]	$2^{m-3} - E/8$	$2^{m-3} + E/8 - 2^{(m-3)/2}$
$m = 4h + 1$	$= 8s + 5$	$= 8s + 1$
N_1 [16]	$2^{m-2} - 2^{(m-3)/2} - 1$	$2^{m-2} + 2^{(m-3)/2} - 1$
N_2 [4]	$2^{m-2} + 2^{(m-3)/2}$	$2^{m-2} - 2^{(m-3)/2}$
N_3 [0]	$2^{m-3} - E/8$	$2^{m-3} + E/8 - 2^{(m-3)/2}$
N_4 [8]	$2^{m-3} + E/8 + 2^{(m-3)/2}$	$2^{m-3} - E/8$
N_5 [12]	$2^{m-3} + E/8 - 2^{(m-3)/2}$	$2^{m-3} - E/8$
N_6 [20]	$2^{m-3} - E/8$	$2^{m-3} + E/8 + 2^{(m-3)/2}$

Thus the weight of $x \mapsto T_1^m(x^{-1} + ux)$ on $\mathbf{F}_{2^m}$ equals $2^m - w_u$ which implies $w_u = 2^m - \lambda_u$. Now

$$\mathcal{K}(u) = \sum_{x \in \mathbf{F}_{2^m}} (-1)^{T_1^m(x^{-1}+ux)} = 2^m - 2\lambda_u.$$

Thus $\mathcal{K}(u) = -2^m + 2w_u$. The proof is completed since

$$-\left(2^m - 2w_u\right) = -\sum_{j=1}^{2^m} (-1)^{T_1^{2m}(u\gamma^j)}. \qquad \square$$

The weights w_u of C can be computed by means of

$$H(u) = \sum_{y \in \mathcal{G} \setminus \{1\}} (-1)^{T_1^{2m}(yu)}, \quad u \in \mathbf{F}_{2^m}^*,$$

and we know from (15) that $H(u) = -\mathcal{K}(u)$. Consequently, Theorem 3, as well as Table 2, provide some properties of the weights of the code C.

Corollary 6. *For each $t \equiv 0$ modulo 4 in the range $[0, 20]$ we have*

$$H(u) \equiv t \pmod{24} \quad \Leftrightarrow \quad \mathcal{K}(u) \equiv 24 - t \pmod{24}.$$

Consequently, those u such that $H(u) \equiv t$ are described by Theorem 3 and the number of times they occur (for a fixed t) is given by Table 2.

6. On the spectrum of Kloosterman sums

Now we are going to compute for each case of Theorem 3 the number of those a which occur.

Proposition 3. *Let $a \in \mathbf{F}_{2^m}^*$. For any set T, recall that $\#T$ is the cardinality of T. Set*

$$N_1 = \#\{a \mid \mathcal{K}(a) \equiv 16 \ (\mathrm{mod}\ 24)\}$$

and

$$N_2 = \#\{a \mid \mathcal{K}(a) \equiv 4 \pmod{24}\}.$$

Then

$$N_1 = 2^{m-2} + \left(\frac{2}{m}\right)2^{(m-3)/2} - 1 \quad \textit{and} \quad N_2 = 2^{m-1} - 1 - N_1,$$

where $(\frac{2}{m})$ *is the Jacobi symbol given by* (4).

Proof. From Theorem 3: $N_1 = \#\{a \mid \mathrm{Tr}(a) = 0 \text{ and } \mathrm{Tr}(a^{1/3}) = 0\}$. By setting $a = b^3$ (with $b \neq 0$), N_1 is exactly:

$$N_1 = \#\{b \mid \mathrm{Tr}(b^3) = 0 \text{ and } \mathrm{Tr}(b) = 0\}. \tag{16}$$

Similarly N_2 is the number of those b such that $\mathrm{Tr}(b^3) = 1$ and $\mathrm{Tr}(b) = 0$. Since

$$N_1 + N_2 = \#\{b \in \mathbf{F}_{2^m}^* \mid \mathrm{Tr}(b) = 0\} = 2^{m-1} - 1,$$

then $N_2 = 2^{m-1} - 1 - N_1$. Let f be the Boolean function $b \mapsto \mathrm{Tr}(b^3)$ and denote by w the number of times $f(b) = 1$ when $\mathrm{Tr}(b) = 0$. According to (16), $N_1 = 2^{m-1} - w - 1$ (note that we do not take $b = 0$). According to (5), we have $C(1) = 2(2^{m-1} - 2w)$, so that $4w = 2^m - C(1)$. Thus, since $C(1) = (\frac{2}{m})2^{(m+1)/2}$, we get

$$N_1 = 2^{m-1} - 1 - 2^{m-2} + C(1)/4 = 2^{m-2} + \left(\frac{2}{m}\right)2^{(m-3)/2} - 1$$

which completes the proof. □

Now we are going to treat the case where $\mathrm{Tr}(a^{1/3}) = 1$ which is more complicated. We want to compute the N_i as follows stated: for $a \in \mathbf{F}_{2^m}^*$, we define

$$N_3 = \#\{a \mid \mathcal{K}(a) \equiv 0 \pmod{24}\}; \tag{17}$$

$$N_4 = \#\{a \mid \mathcal{K}(a) \equiv 8 \pmod{24}\}; \tag{18}$$

$$N_5 = \#\{a \mid \mathcal{K}(a) \equiv 12 \pmod{24}\}; \tag{19}$$

$$N_6 = \#\{a \mid \mathcal{K}(a) \equiv 20 \pmod{24}\}. \tag{20}$$

Proposition 4. *For any odd m, we have*:

$$N_3 + N_4 = 2^{m-2} - \left(\frac{2}{m}\right)2^{(m-3)/2},$$

$$N_5 + N_6 = 2^{m-2} + \left(\frac{2}{m}\right)2^{(m-3)/2},$$

where $(\frac{2}{m})$ *is given by* (4). *Moreover,*

$$N_3 + N_5 = \begin{cases} 2^{m-2} + 2^{(m-3)/2} & \textit{if } m = 4h + 3, \\ 2^{m-2} - 2^{(m-3)/2} & \textit{if } m = 4h + 1. \end{cases}$$

Proof. Notice that $\sum_{i=3}^{6} N_i = 2^{m-1}$ since this sum equals the cardinality of those a such that $\mathrm{Tr}(a^{1/3}) = 1$. Recall that $C(1) = (\frac{2}{m})2^{(m+1)/2}$. From Theorem 3, setting $a = b^3$ (with $b \neq 0$), we have:

$$N_3 + N_4 = \#\{b \mid \mathrm{Tr}(b^3) = 0 \text{ and } \mathrm{Tr}(b) = 1\}.$$

Let f be the Boolean function $x \mapsto \mathrm{Tr}(x^3)$ and denote by τ the number of x such that $\mathrm{Tr}(x) = 1$ and $f(x) = 1$. From (5), we get:

$$C(1) = -2 \sum_{x \in \mathbf{F}_{2^m},\, \mathrm{Tr}(x)=1} e(x^3) = -2(2^{m-1} - 2\tau).$$

Thus

$$N_3 + N_4 = 2^{m-1} - \tau = 2^{m-1} - 2^{m-2} - C(1)/4 = 2^{m-2} - \left(\frac{2}{m}\right)2^{(m-3)/2}.$$

Since the sum of the N_i is equal to 2^{m-1}, we directly deduce $N_5 + N_6$. Now, because $C(b) \neq 0$ if and only if $\mathrm{Tr}(b) = 1$, we have:

$$N_3 + N_5 = \#\left\{ b \;\middle|\; \begin{array}{l} C(b) > 0 \text{ if } m = 4h+3 \\ C(b) < 0 \text{ if } m = 4h+1 \end{array} \right\}.$$

Hence $N_3 + N_5$ is equal to the number of those b such that $C(b)$ is positive (respectively negative). This number is given by Table 1, completing the proof. □

Now, we are going to compute the N_i defined by (17)–(20). In accordance with Theorem 3, each such N_i depends on m. We have to consider $m = 4h+3$ and $m = 4h+1$ for each i. These cases differ by the value of $e(\beta^3)(\frac{2}{m})$ which is the sign of $C(a^{1/3})$. We will denote this sign by λ_i. Thus we have, according to Theorem 3(2),

$$\begin{aligned} i \in \{3,5\} \quad &\Rightarrow \quad \text{if } m = 4h+3 \text{ then } \lambda_i = 1 \text{ else } \lambda_i = -1, \\ i \in \{4,6\} \quad &\Rightarrow \quad \text{if } m = 4h+3 \text{ then } \lambda_i = -1 \text{ else } \lambda_i = 1. \end{aligned} \tag{21}$$

Lemma 6. *For $i \in \{3,4,5,6\}$, let $\epsilon_i \in \mathbf{F}_2$ and $\lambda_i \in \{\pm 1\}$, where λ_i is given by* (21). *Then*

$$N_i = \#\left\{ \beta \;\middle|\; \mathrm{Tr}(\beta) = 0,\ \mathrm{Tr}(\beta^9 + \beta^3 + 1) = \epsilon_i,\ e(\beta^3)\left(\frac{2}{m}\right) = \lambda_i \right\},$$

where if $i \in \{3,4\}$ then $\epsilon_i = 0$ else $\epsilon_i = 1$.

Proof. With notation of Theorem 3, we set $b = a^{1/3}$, $a \in \mathbf{F}_{2^m}^*$. In accordance with the case (2) of this theorem we have $\mathrm{Tr}(b) = 1$ and for any i:

$$N_i = \#\left\{ b \;\middle|\; \mathrm{Tr}(b) = 1,\ \mathrm{Tr}(b^3) = \epsilon_i,\ e(\beta^3)\left(\frac{2}{m}\right) = \lambda_i \right\},$$

where β is the sole element such that $\mathrm{Tr}(\beta) = 0$ and $b = \beta^4 + \beta + 1$; ϵ_i equals 0 when $i \in \{3,4\}$ and 1 otherwise. Thus the value of N_i, as stated above, is exactly the cardinality of the set of those β such that $\mathrm{Tr}(\beta) = 0$, $\mathrm{Tr}((\beta^4 + \beta + 1)^3) = \epsilon_i$ and $e(\beta^3)(\frac{2}{m}) = \lambda_i$. It remains to compute $\mathrm{Tr}(b^3)$:

$$\begin{aligned}\operatorname{Tr}\big((\beta^4+\beta+1)^3\big) &= \operatorname{Tr}\big((\beta^4+\beta+1)(\beta^8+\beta^2+1)\big)\\ &= \operatorname{Tr}\big(\beta^3+\beta^9+\beta+\beta^3+\beta^3+\beta+1\big)\\ &= \operatorname{Tr}\big(\beta^9+\beta^3+1\big). \qquad \square\end{aligned}$$

From Proposition 4, we know that to compute the N_i given by (17)–(20) is reduced to compute N_3. So, we are going to compute N_3.

Proposition 5. *Set* $E=\sum_{x\in\mathbf{F}_{2^m}} e(x^9+x)$; *$s$ is some nonzero integer. Then*

$$N_3=\begin{cases}2^{m-3}-E/8 & \textit{if } m\in\{8s+7,8s+5\},\\ 2^{m-3}+E/8-(\frac{2}{m})2^{(m-3)/2} & \textit{if } m\in\{8s+3,8s+1\},\end{cases}$$

where $(\frac{2}{m})$ *is given by* (4) *and*

$$E=\begin{cases}\pm 2^{(m+1)/2} & \textit{if } m\not\equiv 0 \ (\mathrm{mod}\ 3),\\ \pm 2^{(m+3)/2} & \textit{otherwise}.\end{cases}$$

Proof. To compute N_3, defined by (17), is to compute those a corresponding to the case of Theorem 3 where $\operatorname{Tr}(a^{1/3})=1$, $\operatorname{Tr}(a)=0$, $C(a^{1/3})>0$ if $m=4h+3$ and $C(a^{1/3})<0$ if $m=4h+1$. As before, set $b=a^{1/3}$ and $b=\beta^4+\beta+1$. Thus, according to Lemma 6,

$$N_3=\#\left\{\beta \;\middle|\; \operatorname{Tr}(\beta)=0,\ \operatorname{Tr}\big(\beta^9+\beta^3+1\big)=0,\ e\big(\beta^3\big)\left(\frac{2}{m}\right)=\lambda_3\right\},$$

where $\lambda_3=1$ if $m=4h+3$ and $\lambda_3=-1$ if $m=4h+1$. This means that $e(\beta^3)=(\frac{2}{m})$ and $-(\frac{2}{m})$, respectively. Using (4) we must count precisely those β such that

$$e\big(\beta^3\big)=\begin{cases}1 & \text{if } m=4h+3=8s+7,\\ -1 & \text{if } m=4h+3=8s+3,\\ 1 & \text{if } m=4h+1=8s+5,\\ -1 & \text{if } m=4h+1=8s+1,\end{cases} \tag{22}$$

where $h=2s+1$ and $h=2s$, respectively, for each form of m. Then

$$N_3=\frac{1}{8}\sum_{\beta\in\mathbf{F}_{2^m}}\big(1+e(\beta)\big)\big(1-e\big(\beta^9+\beta^3\big)\big)\big(\lambda e\big(\beta^3\big)+1\big),$$

where λ depends on m only; it is the sign of $e(\beta^3)$ given in (22). So

$$\begin{aligned}8N_3 = 2^m &+\sum_\beta e(\beta)+\lambda\sum_\beta e\big(\beta^3\big)-\sum_\beta e\big(\beta^9+\beta^3\big)-\sum_\beta e\big(\beta^9+\beta^3+\beta\big)\\ &-\lambda\sum_\beta e\big(\beta^9\big)+\lambda\sum_\beta e\big(\beta^3+\beta\big)-\lambda\sum_\beta e\big(\beta^9+\beta\big).\end{aligned}$$

Using Lemma 4 and Example 1 the sums of $e(\beta)$, $e(\beta^3)$, $e(\beta^9)$ and $e(\beta^9+\beta^3+\beta)$ equal zero. On the other hand, the sum of $e(\beta^9+\beta^3)$ is obviously equal to those of $e(\beta^3+\beta)$. Thus, we get

$$8N_3=2^m+(\lambda-1)C(1)-\lambda\sum_\beta e\big(\beta^9+\beta\big).$$

Table 3
Divisibility of $\mathcal{K}(a)$, $a \neq 0$, computed on $\mathbf{F}_{2^9}$

$\mathcal{K}(a)$ (mod 24)	Number it occurs
0	$N_3 = 48$
4	$N_2 = 120$
8	$N_4 = 72$
12	$N_5 = 72$
16	$N_1 = 135$
20	$N_6 = 64$

Since $C(1) = (\frac{2}{m})2^{(m+1)/2}$ and replacing λ by its value given by (22), we obtain the expected expression of N_3.

As recalled in Section 2.2, $E = S(3,1,1)$. When b runs through $\mathbf{F}_{2^m}$, we have: $S(3,1,b) \in \{0, \pm 2^{(m+3)/2}\}$ if 3 divides m and $S(3,1,b) \in \{0, \pm 2^{(m+1)/2}\}$ otherwise. Particularly $S(3,1,1)$ cannot be zero. Indeed, let f be the Boolean function $x \mapsto \mathrm{Tr}(x^9 + x)$ on $\mathbf{F}_{2^m}$ and take any $u \in \mathbf{F}_{2^m}^*$. Then

$$f(x) + f(x+u) = \mathrm{Tr}\big(x^8 u + x u^8 + u^9 + u\big) = \mathrm{Tr}\big(\big(u^{2^{m-3}} + u^8\big)x\big) + \mathrm{Tr}\big(u^9 + u\big).$$

The function $x \mapsto f(x) + f(x+u)$ is constant if and only if $u^{2^6} + u = 0$. This is possible if and only if $\gcd(m,6) = \gcd(m,3) = 3$. But in this case $u^8 = u$ and then $\mathrm{Tr}(u^9 + u) = 0$. We deduce that for any u the function $x \mapsto f(x) + f(x+u)$ cannot be equal to 1. From Lemma 4, it cannot be balanced, i.e., $E \neq 0$, completing the proof. □

Explanation of Tables 2 and 3: The values of the N_i are computed in Table 2. This table includes the number of those a occurring in each case described by Theorem 3. Recall that m is odd and $m \geqslant 5$. The N_i are precisely defined by Proposition 3, (17)–(20). In Table 2, we use the next notation:

$$N_i[\nu] = \#\big\{a \;\big|\; \mathcal{K}(a) \equiv \nu \pmod{24}\big\}.$$

Notation E is used for the sum: $E = \sum_{x \in \mathbf{F}_{2^m}} e(x^9 + x)$. The knowledge of the sign of E for each kind of m in Table 2 would give the precise values of the N_i (see Proposition 5).

As an example, we compute separately the N_i for $m = 9$. In this case $E = \sum_{x \in \mathbf{F}_{2^9}} e(x^9 + x) = -64$. These results are given in Table 3 and can be checked by means of Table 2. Note that $m = 8 + 1$ ($s = 1$ in Table 2).

Acknowledgments

The authors thank the anonymous reviewers who, by a number of comments and suggestions, contributed to improving the manuscript.

Appendix

We compute here the Kloosterman sums for $m = 5$ and $m = 7$ but also the values of the exponential sums G and C, according to (7). For $a \in \mathbf{F}_{2^m}^*$ with $\mathrm{Tr}(a^{1/3}) = 1$, we denote by β one

Table 4
$m = 5$; $p(x) = x^5 + x^2 + 1$

$a^{1/3}$	$\mathrm{Tr}(a^{1/3})$	a	$\mathrm{Tr}(a)$	β	g	$\mathrm{Tr}(g)$	$\mathcal{K}$	C	G
1	1	1	1	0	0	0	12	−8	−8
α	0	α^3	1	$*$	$*$	$*$	4	0	−8
α^3	1	α^9	1	α^2	α^{12}	1	−4	8	8
α^5	1	α^{15}	0	α^{14}	α^9	1	8	8	0
α^7	0	α^{21}	1	$*$	$*$	$*$	4	0	8
α^{11}	1	α^2	0	α^3	α^{30}	0	0	−8	0
α^{15}	0	α^{14}	0	$*$	$*$	$*$	−8	0	0

Table 5
$m = 7$; $p(x) = x^7 + x^3 + 1$

$a^{1/3}$	$\mathrm{Tr}(a^{1/3})$	a	$\mathrm{Tr}(a)$	β	g	$\mathrm{Tr}(g)$	$\mathcal{K}$	C	G
1	1	1	1	0	0	0	−12	16	−40
α	0	α^3	0	$*$	$*$	$*$	16	0	0
α^3	0	α^9	0	$*$	$*$	$*$	−8	0	0
α^5	0	α^{15}	1	$*$	$*$	$*$	4	0	8
α^7	1	α^{21}	1	α^{30}	α^{28}	1	20	−16	8
α^9	0	α^{27}	1	$*$	$*$	$*$	−20	0	−8
α^{11}	1	α^{33}	0	α^{66}	α^{21}	1	−16	−16	16
α^{13}	0	α^{39}	0	$*$	$*$	$*$	−8	0	−16
α^{15}	1	α^{45}	0	α^{22}	α^{31}	1	8	−16	−16
α^{19}	1	α^{57}	1	α^{51}	α^{112}	1	−4	−16	8
α^{21}	1	α^{63}	0	α^{23}	α	0	0	16	16
α^{23}	1	α^{69}	1	α^{38}	α^{81}	0	12	16	−8
α^{27}	1	α^{81}	0	α^{112}	α^{81}	0	0	16	0
α^{29}	0	α^{87}	0	$*$	$*$	$*$	−8	0	0
α^{31}	1	α^{93}	1	α^{16}	α^{119}	0	−12	16	−8
α^{43}	0	α^2	0	$*$	$*$	$*$	16	0	0
α^{47}	0	α^{14}	1	$*$	$*$	$*$	4	0	24
α^{55}	1	α^{38}	1	α^{52}	α^{18}	0	12	16	8
α^{63}	0	α^{62}	1	$*$	$*$	$*$	4	0	−8

of the two elements in $\mathbf{F}_{2^m}$ such that $a^{1/3} = \beta^4 + \beta + 1$. In Tables 4 and 5, the results are given for a set of representatives of the cyclotomic cosets only (since it is the same for all elements from such coset). The star * is given to separate the cases with $\mathrm{Tr}(a^{1/3}) = 0$, i.e., when there is no β such that $a^{1/3} = \beta^4 + \beta + 1$.

For short, we use the following notation: $g = \beta^3 + \beta$, $\mathcal{K} = \mathcal{K}(a)$, $C = C(a^{1/3})$ and $G = G(a)$.

The Jacobi symbol is equal to -1 for $m = 5$ and to 1 for $m = 7$. We denote by p the primitive polynomial generating $\mathbf{F}_{2^m}$.

References

[1] P. Camion, B. Courteau, A. Montpetit, The weight enumerators of the extremal self-dual binary codes of length 32, in: Proceedings of EUROCODE '92, in: CISM Courses and Lectures, vol. 339, Springer-Verlag, 1993, pp. 17–30.

[2] A. Canteaut, C. Carlet, P. Charpin, C. Fontaine, On cryptographic properties of the cosets of $R(1,m)$, IEEE Trans. Inform. Theory 47 (4) (2001) 1494–1513.

[3] L. Carlitz, Explicit evaluation of certain exponential sums, Math. Scand. 44 (1979) 5–16.

[4] P. Charpin, V.A. Zinoviev, On coset weight distributions of the 3-error-correcting BCH-codes, SIAM J. Discrete Math. 10 (1) (February 1997) 128–145.

[5] P. Charpin, T. Helleseth, V. Zinoviev, On cosets of weight 4 of binary BCH codes of length 2^m (m odd), with minimal distance 8, and exponential sums, Probl. Inf. Transm. 41 (4) (2005) 331–348.

[6] P. Charpin, T. Helleseth, V.A. Zinoviev, On binary BCH codes with minimal distance 8 and Kloosterman sums, in: Proceedings of Ninth Int. Workshop on Algebraic and Combinatorial Coding Theory, Kranevo, Bulgaria, 19–25 June, 2004, pp. 90–95.

[7] P. Charpin, T. Helleseth, V.A. Zinoviev, The coset distribution of triple-error-correcting binary primitive BCH codes, in: Proceedings 2005 IEEE International Symposium on Information Theory, ISIT '05, Adelaide, Australie, September 2005.

[8] J.F. Dillon, Elementary Hadamard difference sets, in: Proc. 6th S–E Conf. Combinatorics, Graph Theory, and Computing, Congr. Numer 14 (1975) 237–249.

[9] T. Helleseth, V.A. Zinoviev, On Z_4-linear Goethals codes and Kloosterman sums, Des. Codes Cryptogr. 17 (1–3) (1999) 246–262.

[10] T. Helleseth, P.V. Kumar, Sequences with low correlation, in: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, Part 3: Applications, Elsevier, Amsterdam, 1998, R.A. Brualdi (assistant Ed.) (Chapter 21).

[11] G. Lachaud, J. Wolfmann, The weights of the orthogonals of the extended quadratic binary Goppa codes, IEEE Trans. Inform. Theory 36 (3) (May 1990) 686–692.

[12] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error Correcting Codes, North-Holland, 1986.

[13] R.J. McEliece, Finite Fields for Computer Scientists and Engineers, Kluwer, Boston, 1987.

[14] J.C.C.M. Remijn, H.J. Tiersma, A duality theorem for the weight distribution of some cyclic codes, IEEE Trans. Inform. Theory 34 (5) (September 1988) 1348–1351.