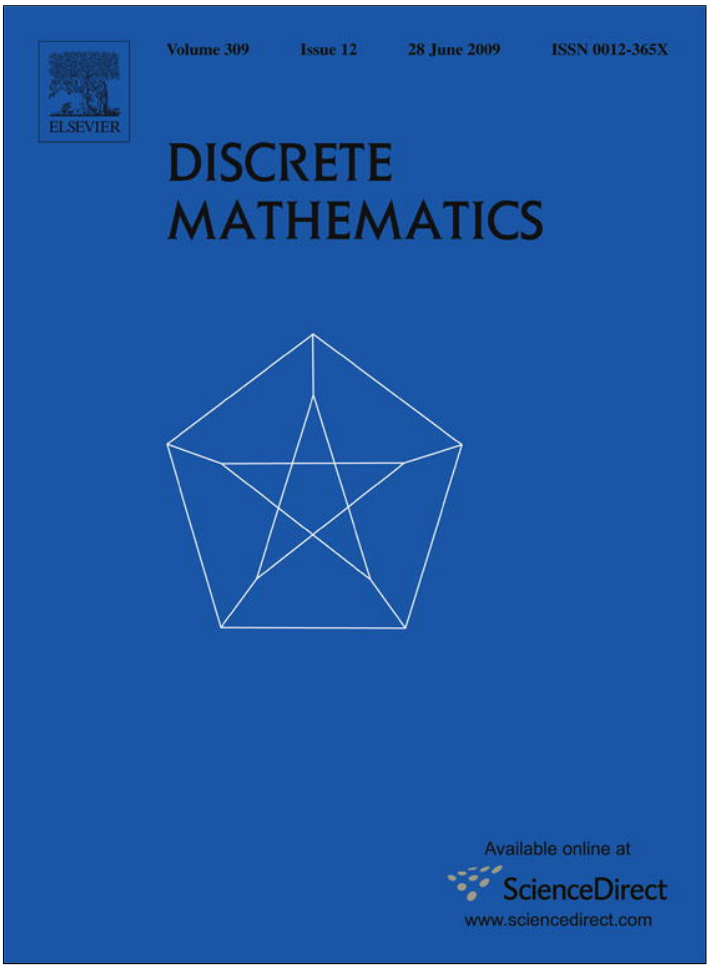

Discrete Mathematics 309 (2009) 3975–3984

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Divisibility properties of classical binary Kloosterman sums☆

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

[a] INRIA, Domaine de Voluceau-Rocquencourt, BP 105 - 78153, Le Chesnay, France

[b] The Selmer Center, Department of Informatics, University of Bergen, PB 7803, N-5020, Bergen, Norway

[c] Institute for Problems of Information Transmission of the Russian Academy of Sciences, Bol'shoi Karetnyi per. 19, GSP-4, Moscow, 101447, Russia

ARTICLE INFO

Article history:
Received 11 December 2007
Received in revised form 17 October 2008
Accepted 7 November 2008
Available online 20 December 2008

Keywords:
Binary primitive narrow sense BCH code
Coset
Coset weight distribution
Exponential sum
Cubic sum
Classical Kloosterman sum
Inverse cubic sum
Partial sum

ABSTRACT

Let $K(a)$ be the so-called classical Kloosterman sum over $\mathbf{F}_{2^m}$. In this paper, we compute $K(a)$ modulo 24 for even m, completing our previous results for odd m. We extensively study the links between $K(a)$ and other exponential sums, especially the cubic sums. We point out (as we did for odd m) that the values $K(a)$ are involved in the computation of the weight distributions of cosets of primitive narrow sense extended BCH codes of length 2^m and minimum distance 8. We also complete some recent results on $K(a) - 1$ modulo 3.

1. Introduction

We denote by $K(a)$, $a \in \mathbf{F}_{2^m}$, the so-called classical binary Kloosterman sum over $\mathbf{F}_{2^m}$. Let B_m be the extended binary narrow sense BCH code of length 2^m and minimum distance 8 and $D^{(4)}$ be any coset of B_m of minimum weight 4. Recall that the vectors of weight 4 in $D^{(4)}$ are the *coset leaders*. We continue here our work on coset weight distributions of B_m (see [6, 3–5]) and on the relations which link the weight distribution of any coset $D^{(4)}$ with the spectrum of three exponential sums, including the Kloosterman sum. In [4], we computed the spectrum of $K(a)$ modulo 24 in the case where m is odd. We obtained this result by using some congruences modulo 3, which we derived from our study of the cosets $D^{(4)}$, for m odd.

Most recently, we treated the even case (m even) and found the exact expression for the number of coset leaders of any coset $D^{(4)}$ [5]. We proved that, as for the odd case, this expression includes exponential sums of three different types: Kloosterman sums, cubic sums and inverse cubic sums, over $GF(2^m)$. As often, the even case is much harder, *i.e.*, the expressions are more complicated as well as the spectrum of the cubic sum is. This led us to another approach, independent from the codes B_m; it appeared that this approach is suitable for odd m too.

The paper is organized as follows: Section 2 includes the definitions and basic properties which we need for the remainder of the paper. Most of these properties are known and given without proof. By Lemma 8, we exhibit some relations between $K(a)$ and partial cubic sums which are particularly important in the even case. In Section 3, we recall our main result concerning cosets $D^{(4)}$ of B_m [3,5] and show how we can extend our previous results (for odd m) to any m. Section 4 is

☆ This work was supported by INRIA-Rocquencourt, by the Norwegian Research Council and also by the Russian fund of fundamental researches (the number of project 06 - 01 - 00226).

* Corresponding author.
E-mail address: zinov@iitp.ru (V. Zinoviev).

0012-365X/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2008.11.010

devoted to the congruences modulo 3, and further modulo 24, which prepare the complete result, for even m, of the next section. Our main results are given in Section 5, where we compute $K(a)$ modulo 24 by means of the values of the cubic sums. In particular, we show the links between $K(a)$ modulo 3 and the pair of cubic sums $(C(a), C(a, a))$ by Theorem 18.

In the last section, we study the divisibility of $K(a) - 1$ by 3. Notably, we complete the results presented in [8].

2. Preliminaries

In this paper $\mathbf{F}_{2^m}$ always denotes the Galois field of order 2^m where $m \geq 3$. We use the notation $e(p(x)) = (-1)^{\mathrm{Tr}(p(x))}$ where Tr is the absolute trace over $\mathbf{F}_{2^m}$, and $e(a)$ is an additive character of $\mathbf{F}_{2^m}$. For even m, we will also use the trace function from $\mathbf{F}_{2^m}$ to its subfield $\mathbf{F}_4$, denoted by T_2^m, that is

$$T_2^m(x) = x + x^4 + x^{4^2} + \cdots + x^{4^{s-1}} \quad \text{where } m = 2s.$$

For any set V, $V^* = V \setminus \{0\}$ and the cardinality of V is denoted by $\#V$.

2.1. Equations of low degree

Lemma 1 ([1]). *The cubic equation $x^3 + ax + b = 0$, where $a, b \in \mathbf{F}_{2^m}^*$ has a unique solution in $\mathbf{F}_{2^m}$ if and only if $Tr(a^3/b^2) \neq Tr(1)$. Furthermore, if it has three distinct roots in $\mathbf{F}_{2^m}$, then $Tr(a^3/b^2) = Tr(1)$.*

Lemma 2 ([10]). *Let $m \geq 2$ be an integer. Set $f_b(x) = x^3 + x + b$, for any $b \in \mathbf{F}_{2^m}^*$. Then f_b has 0, 1 or 3 roots in $\mathbf{F}_{2^m}$. Let*

$$M_i = \#\{b : f_b(x) = 0 \text{ has precisely } i \text{ solutions in } \mathbf{F}_{2^m}\}.$$

If m is odd, then

$$M_0 = (2^m + 1)/3, \qquad M_1 = 2^{m-1} - 1 \quad \text{and} \quad M_3 = (2^{m-1} - 1)/3.$$

If m is even, then

$$M_0 = (2^m - 1)/3, \qquad M_1 = 2^{m-1} \quad \text{and} \quad M_3 = (2^{m-1} - 2)/3.$$

The next lemma will be useful, in particular for the understanding of Theorem 5 (below). We give the proof for clarity.

Lemma 3. *Let m be even. Set $f_c(x) = x^4 + cx + 1$, with $c \in \mathbf{F}_{2^m}^*$. Let*

$$N_i = \#\{c \in \mathbf{F}_{2^m}^* : f_c(x) = 0 \text{ has precisely } i \text{ solutions in } \mathbf{F}_{2^m}\}.$$

Then f_c has 0, 1 or 4 roots in $\mathbf{F}_{2^m}$. Precisely,

- *f_c has only one root if and only if c is not a cube;*
- *when $c = b^3$, for some b,*
  f_c has no root if $T_2^m(1/b) \neq 0$;
  f_c has 4 roots if $T_2^m(1/b) = 0$.

Moreover

$$N_0 = 2^{m-2}, \qquad N_1 = 2(2^m - 1)/3, \qquad N_4 = (2^{m-2} - 1)/3.$$

Proof. Note that f_c is an affine mapping on $\mathbf{F}_{2^m}$. More precisely,

$$f_c(x) = \ell_c(x) + 1 \quad \text{with } \ell_c(x) = x^4 + cx,$$

where ℓ_c is linear on $\mathbf{F}_{2^m}$. So, if f_c has at least one root, say z, then the number of roots of f_c equals the number of roots of ℓ_c. This is because for any root x of ℓ_c, we have

$$f_c(z + x) = f_c(z) + \ell_c(x) = 0.$$

Let $P_3 = \{b^3 \mid b \in \mathbf{F}_{2^m}^*\}$. Note that P_3 has cardinality $(2^m - 1)/3$. Since $\ell_c(x) = x(x^3 + c)$, the mapping ℓ_c is a permutation if and only if $c \notin P_3$. Otherwise ℓ_c has four roots which are 0 and the three elements $(b, b\delta, b\delta^2)$, where $c = b^3$ and δ is an element of $\mathbf{F}_4$ of order 3. Clearly $N_2 = N_3 = 0$.

When ℓ_c is a permutation, there is only one x such that $\ell_c(x) = 1$. This means that f_c has only one root if and only if $c \notin P_3$, providing $N_1 = 2(2^m - 1)/3$.

Now suppose that $c = b^3$ for some $b \in \mathbf{F}_{2^m}^*$. In this case, either f_c has no root or f_c has 4 roots. Replacing $x = by$, to solve $f(x) = 0$ is to solve

$$y^4 + y + \frac{1}{b^4} = 0. \tag{1}$$

The image set of $y \mapsto y^4 + y$ has exactly $2^{m-2} - 1$ non zero elements, corresponding to those b such that (1) has four solutions. Since $c = b^3$, we get $(2^{m-2} - 1)/3$ elements c such that f_c has four roots. In this case, b satisfies

$$T_2^m\left(\frac{1}{b}\right) = T_2^m(y^4 + y) = 0.$$

Moreover, if $T_2^m(1/b) \neq 0$ then (1) is not satisfied. We can conclude $N_4 = (2^{m-2} - 1)/3$ and, further,

$$N_0 = 2^m - 1 - \frac{2^{m-2} - 1 + 2^{m+1} - 2}{3} = 2^m - \frac{3 \cdot 2^m}{4} = 2^{m-2}. \quad \square$$

2.2. Some exponential sums

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

Definition 4. The classical Kloosterman sums are:

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

The cubic sums are:

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

We denote $C(a, 0)$ by $C(a)$. The *inverse cubic* sums are:

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

The partial cubic sums are:

$$P(a, b) = \sum_{x \in \mathbf{F}_{2^m}:\ Tr(1/x)=0} e(ax^3 + bx), \quad a \in \mathbf{F}_{2^m}^*, b \in \mathbf{F}_{2^m}.$$

The Kloosterman sums and the inverse cubic sums are generally defined on $\mathbf{F}_{2^m}^*$, the multiplicative group of $\mathbf{F}_{2^m}$. In this paper we extend them to 0, assuming that

$$e(x^{-1}) = e(x^{-3}) = 1 \text{ for } x = 0.$$

In fact: $Tr(x^{-1}) = Tr(x^{2^{m-1}-1})$ and $Tr(x^{-3}) = Tr(x^{2^{m-2}-1})$. It is well known that for even m and for any $a \in \mathbf{F}_{2^m}$ we have

$$-2^{(m/2)+1} + 4 \leq K(a) \leq 2^{(m/2)+1}. \tag{2}$$

Also, for any pair (a, b) of nonzero elements of $\mathbf{F}_{2^m}$, we have

$$|G(a, b)| \leq 2^{m/2+2}. \tag{3}$$

These bounds are explained in [5].

The spectrum of the cubic sum $C(a, b)$ was first specified by Carlitz [2]. In this paper we use the sums $C(a, a)$ and $C(a)$ only. For even m, $m = 2s$, the next theorem is directly deduced from [2, Theorem 1]. Recall that $C(a) = C(a, 0)$.

Theorem 5. *Let $a \in \mathbf{F}_{2^m}^*$. For any even $m = 2s$ we have that*

$$C(a) = \begin{cases} (-1)^{s+1}2^{s+1}, & \text{if } a \text{ is a cube in } \mathbf{F}_{2^m}, \\ (-1)^s 2^s, & \text{otherwise.} \end{cases}$$

If $a = b^3, b \in \mathbf{F}_{2^m}^*$, then

$$C(a, a) = \begin{cases} 0, & \text{if } T_2^{2s}(b) \neq 0, \\ (-1)^{s+1}2^{s+1}e(x_0^3), & \text{otherwise,} \end{cases}$$

where x_0 denotes any solution of $x^4 + x = b^4$.

If $a \neq b^3$, then for all such $a \in \mathbf{F}_{2^m}^*$

$$C(a, a) = e\left(\frac{1}{h+1}\right)(-1)^s 2^s,$$

where h is the unique solution of $ax^4 + x + a = 0$.

2.3. Useful properties

Lemma 6 ([9]). *For any $m \geq 3$*

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

Lemma 7 ([5]). *For any $a \in \mathbf{F}_{2^m}^*$ and any $m \geq 3$:*

$$K(a) = 2 \sum_{x, Tr(1/x)=0} e(ax) = -2 \sum_{x, Tr(1/x)=1} e(ax),$$

where x runs through $\mathbf{F}_{2^m}$.

Lemma 8 ([5]). *Let $a \in \mathbf{F}_{2^m}^*$. Then we have*

- *$2P(a, a) = K(a)$ when m is odd;*
- *$2P(a, a) = 2\,C(a, a) + K(a)$ when m is even.*

3. Some systems of BCH equations

Recall that B_m is the binary extended (primitive narrow sense) BCH code of length $n = 2^m$ where $m \geq 5$, with minimum distance 8. The number of coset leaders of any coset $D^{(4)}$ (of minimum weight 4) of B_m is the number of solutions $\{x, y, z, u\}$ of the following system of equations over $\mathbf{F}_{2^m}$:

$$\left.\begin{array}{rcl} x + y + z + u &=& a \\ x^3 + y^3 + z^3 + u^3 &=& b \\ x^5 + y^5 + z^5 + u^5 &=& c \end{array}\right\}. \tag{4}$$

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, with $a \neq 0$. Let $\mu(a, b, c)$ be the number of solutions of (4) over $\mathbf{F}_{2^m}$ for $m \geq 3$. Then there are $\epsilon \in \mathbf{F}_2$ and $\lambda \in \mathbf{F}_{2^m}^*$

$$\epsilon = Tr\left(\frac{b}{a^3}\right) \quad \text{and} \quad \lambda = \frac{c}{a^5} + \frac{b^2}{a^6} + \frac{b}{a^3} + 1, \tag{5}$$

such that $\mu(a, b, c)$ equals the value $\mu(\epsilon, \lambda)$, which is given in the next theorem.

Theorem 9. *For $m \geq 3$ the value $\mu(\epsilon, \lambda)$, where λ and ϵ are given by (5), is an even integer expressed as follows.*

- *For even m* [5]

$$24\,\mu(\epsilon, \lambda) = 2^m - 8 + 3 \cdot G(\lambda, \lambda) + C(\lambda) + (-1)^{\epsilon}\,(2K(\lambda) + 4C(\lambda, \lambda) - 8)\,. \tag{6}$$

- *For odd m* [3]

$$24\,\mu\,(\epsilon, \lambda) = 2^m - 8 + 3 \cdot G(\lambda, \lambda) + (-1)^{\epsilon+1}\,(2K(\lambda) + 2C(\lambda, \lambda) - 8)\,. \tag{7}$$

- *Furthermore, when $\lambda = 0$ then $\mu(\epsilon, 0) = 0$ for even and odd m.*

Remark 10. For $a \neq 0$ and odd m, it is easy to see that $C(a, a) = C(1, b)$ where $a = b^3$. Indeed, such b exists for any a and we have

$$C(a, a) = \sum_{x \in \mathbf{F}_{2^m}} e(ax^3 + ax) = \sum_{y \in \mathbf{F}_{2^m}} e(y^3 + by) = C(1, b) \tag{8}$$

where $x = y/b$. Thus, $C(1, \lambda^{1/3})$ could replace $C(\lambda, \lambda)$ in (7), as it was made in the formula (19) of [3].

Now we deduce two important corollaries from Theorem 9. Note that we tried to establish Corollary 12 directly (without Theorem 9) without success.

Corollary 11. *For any $m \geq 8$, any $\epsilon \in \mathbf{F}_2$ and any $\lambda \in \mathbf{F}_{2^m}^*$, the number at the right hand side of the equality (6) (resp. (7)) is a positive integer divisible by 48.*

Proof. We assume that m is even, $m = 2s$, since the case where m is odd was already proved in [4]. We denote by A_m the number at the right hand side of (6):

$$A_m = 2^m - 8 + 3G(\lambda, \lambda) + C(\lambda) + (-1)^\epsilon \cdot (2K(\lambda) + 4C(\lambda, \lambda) - 8)\,.$$

Since $\mu(\epsilon, \lambda)$ is even (Theorem 9), A_m is a multiple of 48. Now we use Theorem 5 and the bounds given by (2) and (3). We get:

$$\begin{aligned} A_m &\geq 2^m - 8 - 3 \cdot 2^{s+2} - 2^{s+1} - (2^{s+2} + 2^{s+3} + 8) \\ &\geq 2^m - 16 - 26 \cdot 2^s. \end{aligned}$$

Hence $A_m > 0$ when $2^s(2^s - 26) > 16$ providing that $A_m > 0$ as soon as $s \geq 5$. The case $m = 8$ has been checked by overall calculations of all possible values of $\mu(\epsilon, \lambda)$ (see [5]). □

Corollary 12. *Let $\lambda \in \mathbf{F}_{2^m}^*$, where m is any integer such that $m \geq 5$. Then $G(\lambda, \lambda)$ is divisible by 8 for any m and any λ. Moreover:*

$$G(\lambda, \lambda) \equiv \begin{cases} 8 \pmod{16}, & \text{if } Tr(\lambda) = 1, \\ 0 \pmod{16}, & \text{if } Tr(\lambda) = 0, \end{cases} \tag{9}$$

with one exceptional case when $m = 6$ and λ is a not cube.

Proof. We already proved the case where m is odd in [4, Lemma 5]. So, we assume that m is even, $m = 2s$ with $s \geq 3$. First, it is clear that $G(\lambda, \lambda)$ is divisible by 8 for any $\lambda \in F^*$ and any $m \geq 6$. This comes directly from the formula (6) in Theorem 9. Note that the value $K(\lambda)$ is a multiple of 4, for any $\lambda \in \mathbf{F}_{2^m}^*$. Moreover, from Theorem 5, $C(\lambda)$ and $C(\lambda, \lambda)$ are divisible by 8 as soon as $s \geq 3$.

The cubic sums $C(\lambda)$ and $C(\lambda, \lambda)$ are congruent to 0 modulo 2^{s+1} when λ is a cube. Thus, they are congruent to 0 modulo 16 as soon as $s \geq 3$ which is $m \geq 6$. Hence, according to (6), $G(\lambda, \lambda)$ is divisible by 16 as soon as $K(\lambda)$ is divisible by 8. Applying Lemma 6, the first part of the proof is completed.

When λ is not a cube, the cubic sums $C(\lambda)$ and $C(\lambda, \lambda)$ take the values $\pm 2^s$ only. If $s \geq 4$ then, as previously, (9) holds. Computing all $\mu(\epsilon, \lambda)$ for $m = 6$ in [5], we noticed that (9) does not hold in this case. □

Together with the previous corollaries, we directly obtain the following congruence linking Kloosterman sums and cubic sums.

Corollary 13. *Let $m \geq 8$ be any integer and let $\lambda \in \mathbf{F}_{2^m}^*$. Set*

$$B_m(\epsilon, \lambda) = 24 \cdot \mu(\epsilon, \lambda) - 3 \cdot G(\lambda, \lambda),$$

where $\mu(\epsilon, \lambda)$ is given by (6) for even m and by (7) for odd m. Then for any $\epsilon \in \mathbf{F}_2$, we have

$$B_m(\epsilon, \lambda) \equiv \begin{cases} 0 \pmod{48}, & \text{if } Tr(\lambda) = 0, \\ 24 \pmod{48}, & \text{if } Tr(\lambda) = 1. \end{cases}$$

4. More congruence relations

In this section, we establish some congruences which could be obtained from the results of the previous section. We used this last method for odd m: in [4], we computed $K(a) \pmod 3$ by means of our results on 3-error-correcting BCH codes of length 2^m, m odd.

We here use the relations linking Kloosterman sums to the partial sums $P(a, a)$. Then the main congruences presented in Theorem 15 (below) for any m can be obtained directly.

Lemma 14. *Let $m \geq 5$ and $a \in \mathbf{F}_{2^m}^*$. Set, summing over $x \in \mathbf{F}_{2^m} \setminus \{0, 1\}$,*

$$A = \sum_{x, Tr(1/x)=0} e(a(x^3 + x)) \quad \text{and} \quad B = \sum_{x, Tr(1/x)=1} e(a(x^3 + x)).$$

Then, 3 divides A when m is even and 3 divides B when m is odd.

Proof. Note that for $x \in \mathbf{F}_{2^m} \setminus \{0, 1\}$

$$Tr\left(\frac{1}{x^3 + x}\right) = Tr\left(\frac{1}{x^2 + 1} + \frac{1}{x + 1} + \frac{1}{x}\right) = Tr\left(\frac{1}{x}\right). \tag{10}$$

Let m be even. Since $Tr(0) = Tr(1) = 0$, the sum A has exactly $2^{m-1} - 2$ terms. According to Lemma 1, for any c such that $Tr(1/c) = 0$ there is either zero or three x satisfying $x^3 + x = c$. Thus, using (10),

$$A = 3\sum_{c\in I} e(ac), \quad I = \{c \mid c \neq 0, c = x^3 + x \text{ with } Tr(1/x) = 0\}.$$

Now, assume that m is odd. In this case, $Tr(0) = 0$ while $Tr(1) = 1$. The sum B has $2^{m-1} - 1$ terms and for any c such that $Tr(1/c) = 1$ there is either zero or three x satisfying $x^3 + x = c$. Thus, using (10),

$$B = 3\sum_{c\in I} e(ac), \quad I = \{c \mid c \neq 0, c = x^3 + x \text{ with } Tr(1/x) = 1\}. \quad \square$$

Theorem 15. *Let $a \in \mathbf{F}_{2^m}^*$. Then the following congruences hold.*

- *If m is odd then $K(a) \equiv 1 - C(a, a) \pmod 3$.*
- *If m is even then $K(a) \equiv 1 + C(a, a) \pmod 3$.*

Proof. First, we need the following formula:

$$\begin{aligned} C(a, a) &= \sum_{x\in\mathbf{F}_{2^m}} e(a(x^3 + x)) \\ &= \sum_{x,Tr(1/x)=0} e(a(x^3 + x)) + \sum_{x,Tr(1/x)=1} e(a(x^3 + x)) \\ &= P(a, a) + \sum_{x,Tr(1/x)=1} e(a(x^3 + x)). \end{aligned} \tag{11}$$

Let m be odd. Then, using Lemma 8, and (11),

$$K(a) = 2P(a, a) = 2C(a, a) - 2\sum_{x,Tr(1/x)=1} e(a(x^3 + x)).$$

But the sum above on the right is equal to $B + 1$ where B is divisible by 3 (see Lemma 14). Then

$$K(a) \equiv 2(C(a, a) - 1) \pmod 3,$$

which gives the statement.

Now assume that m is even. Using Lemma 8 again, we get

$$K(a) = 2P(a, a) - 2C(a, a).$$

Here $P(a, a)$ is equal to $A + 2$ where A is divisible by 3 (see Lemma 14). Hence

$$K(a) \equiv 4 - 2\,C(a, a) \equiv 1 + C(a, a) \pmod 3. \quad \square$$

The next theorem is our main congruence modulo 24. From now on, we treat the even case only. Recall that the case where m is odd was presented in [4].

Theorem 16. *Let $m = 2s$ with $s \geq 3$. Let $a \in \mathbf{F}_{2^m}^*$. Then we have:*
If $Tr(a) = 0$ then

$$K(a) - C(a, a) \equiv 16 \pmod{24} \tag{12}$$

else

$$K(a) - C(a, a) \equiv 4 \pmod{24}. \tag{13}$$

Proof. Recall that for even m, we have for any $a \in \mathbf{F}_{2^m}^*$

$$K(a) - C(a, a) \equiv 1 \pmod 3, \tag{14}$$

from Theorem 15. Now, we use the result of Carlitz [2], a simpler form of which is given by Theorem 5. It implies that $C(a, a) \equiv 0$ modulo 8 as soon as $s \geq 3$, that is $m \geq 6$. So, in this case

$$K(a) - C(a, a) \equiv K(a) \pmod 8.$$

Set $L(a) = K(a) - C(a, a)$ and apply Lemma 6. If $Tr(a) = 0$ then $K(a) \equiv 0 \pmod 8$ so that $L(a) = 8R$, for some integer R.

This leads to $L(a) \equiv 2R \pmod 3$. According to (14) we get $R \equiv 2 \pmod 3$. Consequently $L(a) \equiv 16 \pmod{24}$.

Similarly, if $Tr(a) = 1$ then $L(a) = 8R+4$, which leads to $L(a) \equiv 2R+1 \pmod 3$. Then, from (14), we obtain $R \equiv 0 \pmod 3$ which implies $L(a) \equiv 4 \pmod{24}$, completing the proof. $\square$

5. Kloosterman sums modulo 24 and cubic sums

In this section we compute $K(a) \pmod{24}$. Moreover we obtain some relations between $K(a)$, $C(a)$ and $C(a, a)$. We wish to point out the interest of these relations, which specify the even case (m even).

We need the following simple observation.

Lemma 17. *Let $r \geq 3$. Then*

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

The next theorem (comparing to [4, Theorem 3]) shows the differences between the even case (m even) and the odd case (m odd).

Theorem 18. *Let $m = 2s$, with $s \geq 2$, and $a \in \mathbf{F}_{2^m}^*$. Let $K(a)$, $C(a)$ and $C(a, a)$ be the exponential sums defined in Section 2.2. Then we have:*

(1) $K(a) \equiv 2 \pmod 3$ *if and only if* $C(a, a) = C(a)$. *In this case*

$$K(a) \equiv \begin{cases} 8 \pmod{24} & \text{if } Tr(a) = 0 \\ 20 \pmod{24} & \text{if } Tr(a) = 1. \end{cases}$$

(2) $K(a) \equiv 0 \pmod 3$ *if and only if* $C(a, a) = -C(a)$. *In this case*

$$K(a) \equiv \begin{cases} 0 \pmod{24} & \text{if } Tr(a) = 0 \\ 12 \pmod{24} & \text{if } Tr(a) = 1. \end{cases}$$

(3) $K(a) \equiv 1 \pmod 3$ *if and only if* $|C(a, a)| \neq |C(a)|$.
In this case $C(a, a) = 0$, $a = b^3$ for some b such that $T_2^m(b) \neq 0$ and

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

Proof. For $m \geq 6$ we apply Theorem 16. Before, we have to specify the divisibility of $C(a)$. From Theorem 5, we know that $C(a) = (-1)^r 2^r$ with $r = s$ or $r = s + 1$. From Lemma 17, we get

$$(-1)^r 2^r \equiv (-1)^r \times (-1)^r 16 \pmod{24},$$

providing $C(a) \equiv 16 \pmod{24}$ for any a.

Assume that $C(a) = C(a, a)$. Then

$$K(a) - C(a, a) = K(a) - C(a) \equiv K(a) - 16 \pmod{24}.$$

Using (12) and (13), we get $K(a) \equiv 8$ if $Tr(a) = 0$ and $K(a) \equiv 20$ otherwise. In both cases, $K(a) \equiv 2 \pmod 3$.

Assume that $C(a) = -C(a, a)$. Then

$$K(a) - C(a, a) = K(a) + C(a) \equiv K(a) + 16 \pmod{24}.$$

Thus, we get $K(a) \equiv 0$ if $Tr(a) = 0$ and $K(a) \equiv 12$ otherwise. In both cases, $K(a) \equiv 0 \pmod 3$.

Finally, if $C(a, a) \notin \{\pm C(a)\}$ then the only possibility is $C(a, a) = 0$, implying $a = b^3$ for some b such that $T_2^m(b) \neq 0$ (see Theorem 5). In this case the divisibility of $K(a)$ is directly obtained from Theorem 16. And this is clearly the case where $K(a) \equiv 1 \pmod 3$.

The case $m = 4$ follows by direct checking of sums $K(a)$, $C(a)$, and $C(a, a)$ for all $a \in \mathbf{F}_{2^m}^*$. □

The link between the set of elements a such that $K(a) = 0$ and the existence of the Dillon difference sets [7] is well known. The previous theorem provides a useful necessary condition.

Corollary 19. *Let $m = 2s$. Let $a \in \mathbf{F}_{2^m}$ such that $K(a) = 0$. Then we have:*
$Tr(a) = 0$, $C(a, a) \neq 0$ and $C(a) = -C(a, a)$.

We can also express $K(a)$ modulo 24 using $C(a, a)$ only.

Theorem 20. *Let $m = 2s$ with $s \geq 2$. Then we have for any $a \in \mathbf{F}_{2^m}^*$:*

- *If $C(a, a) = 0$, then*

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

- *If* $C(a,a) \in \{2^s, -2^{s+1}\}$, *then for odd* s

$$K(a) \equiv \begin{cases} 0 \pmod{24}, & \text{if } Tr(a) = 0, \\ 12 \pmod{24}, & \text{if } Tr(a) = 1, \end{cases}$$

and for even s

$$K(a) \equiv \begin{cases} 8 \pmod{24}, & \text{if } Tr(a) = 0, \\ 20 \pmod{24}, & \text{if } Tr(a) = 1. \end{cases}$$

- *If* $C(a,a) \in \{-2^s, 2^{s+1}\}$, *then for odd* s

$$K(a) \equiv \begin{cases} 8 \pmod{24}, & \text{if } Tr(a) = 0, \\ 20 \pmod{24}, & \text{if } Tr(a) = 1, \end{cases}$$

and for even s

$$K(a) \equiv \begin{cases} 0 \pmod{24}, & \text{if } Tr(a) = 0, \\ 12 \pmod{24}, & \text{if } Tr(a) = 1. \end{cases}$$

Proof. The case $C(a,a) = 0$ is the same as Theorem 18, **(3)**.

Assume that $C(a,a) \in \{2^s, -2^{s+1}\}$. Using Theorem 5, this implies $C(a) \in \{-2^s, 2^{s+1}\}$ when s is odd and $C(a) \in \{2^s, -2^{s+1}\}$ when s is even. Thus we apply Theorem 18, **(2)**, and Theorem 18, **(1)**, respectively.

When $C(a,a) \in \{-2^s, 2^{s+1}\}$, we have similarly $C(a) \in \{-2^s, 2^{s+1}\}$ for odd s and $C(a) \in \{2^s, -2^{s+1}\}$ for even s. Here, we apply Theorem 18, **(1)**, and Theorem 18, **(2)**, respectively. □

To conclude this section, we want to explain the equations $C(a,a) = \pm C(a)$, where $a \in \mathbf{F}_{2^m}^*$.

Lemma 21. *For any even* $m \geq 4$ *and any* $a \in \mathbf{F}_{2^m}^*$ *we have*

$$C(a,a) = \begin{cases} C(a) & \text{when } Tr\left(\dfrac{1}{h+1}\right) = 0, \\ -C(a) & \text{when } Tr\left(\dfrac{1}{h+1}\right) = 1. \end{cases}$$

where $h \in \mathbf{F}_{2^m}$ *is such that*

$$a h^4 + h + a = 0.$$

Proof. Note that obviously $C(a,a) = C(a^2, a^2)$. Clearly, we have for any $h \in \mathbf{F}_{2^m}$:

$$\begin{aligned} C(a) &= \sum_{x \in \mathbf{F}_{2^m}} e(ax^3) = \sum_{x \in \mathbf{F}_{2^m}} e\left(a(x+h)^3\right) \\ &= \sum_{x \in \mathbf{F}_{2^m}} e\left(a(x^3 + x^2 h + x h^2 + h^3)\right) \\ &= \sum_{x \in \mathbf{F}_{2^m}} e\left(ax^3 + x^2(a^2 h^4 + ah) + ah^3\right) \\ &= \sum_{y \in \mathbf{F}_{2^m}} e\left(a^2 y^3 + y(a^2 h^4 + ah) + ah^3\right), \quad \text{where } y = x^2, \\ &= (-1)^{\mathrm{Tr}(ah^3)} C(a^2, a^2 h^4 + ah). \end{aligned} \tag{15}$$

First note that we obtain here all $b \in \mathbf{F}_{2^m}^*$ such that either

$$C(a,b) = C(a) \quad \text{when } Tr(ah^3) = 0$$

or

$$C(a,b) = -C(a) \quad \text{when } Tr(ah^3) = 1.$$

Indeed, according to (15) we can set $b^2 = a^2 h^4 + ah$. The linear mapping $h \mapsto a^2 h^4 + ah$ is a permutation if and only if a is not a cube. Otherwise, its image is of codimension 2. But for any cube a there are exactly 2^{m-2} elements $b \in \mathbf{F}_{2^m}$ such that $C(a,b) \neq 0$ (see [2, Theorem 1]).

Now we consider the sum $C(a,a)$ only, that is the $h \in \mathbf{F}_{2^m}$ such that

$$a^2 h^4 + ah = a^2 \text{ or, equivalently, } ah^4 + h + a = 0.$$

Therefore

$$h^4 + \frac{h}{a} + 1 = 0. \tag{16}$$

When (16) is satisfied for some h_1, we have $a = h_1/(h_1+1)^4$ and

$$Tr(ah_1^3) = Tr\left(\frac{h_1^4}{(h_1+1)^4}\right) = Tr\left(\frac{h_1}{h_1+1}\right) = Tr\left(\frac{1}{h_1+1}\right).$$

Suppose that a is not a cube. There are $2(2^m-1)/3$ such a, where each a corresponds to the only one solution of (16) (see Lemma 3).

When $a = b^3$, to solve (16) is to find the solutions y of

$$y^4 + y + b^4 = 0 \tag{17}$$

(replacing $y = hb$, see (1)). If there is at least one solution of (17) then there are four solutions, say y_i for $i = 1, \ldots, 4$, and $b^4 = y_i^4 + y_i$ for any i. □

As one would expect, the results above are in accordance with Theorem 5.

6. Another divisibility modulo 3

In this section we study the divisibility by 3 of $K(a) - 1$. In [9] it has been proved that for odd m and any a, $a \neq 0, 1$

$$K(a^4 + a^3) - 1 \equiv 0 \pmod 3.$$

In [4], we specified $K(a) - 1$ modulo 3, but for odd m only. Another expression is proposed by [8], also for odd m. For even m and any a $(a \neq 0, 1)$ we have from [9] that $K(a^4 + a^3)$ is congruent to 8 or 0 modulo 12 depending on $Tr(a) = 0$ or $Tr(a) = 1$. Here we give another proof of our previous result (in [4] for odd m) and also completely solve the case of even m, by proving the following theorem.

Theorem 22. *Let a be any element in $\mathbf{F}_{2^m}^*$. Then we have*

- *When m is odd then $K(a) - 1$ is divisible by 3 if and only if $Tr(a^{1/3}) = 0$. This is equivalent to*
$$a = \frac{\beta}{(1+\beta)^4} \quad \text{for some } \beta \in \mathbf{F}_{2^m}^*.$$
- *When $m = 2s$. $K(a) - 1$ is divisible by 3 if and only if*
$$a = b^3 \quad \text{for some } b \text{ such that } T_2^{2s}(b) \neq 0.$$
- *In both cases $K(a) - 1$ is divisible by 3 if and only if $C(a, a) = 0$.*

Proof. Recall that notation K and C for exponential sums is introduced in Definition 4 for any m (odd or even). Also, we set $C(a) = C(a, 0)$ in any case.

Let m be odd, so that $x \mapsto ax^3$ is a permutation. This means notably that $C(a) = 0$, for any $a \in \mathbf{F}_{2^m}^*$. From Theorem 15, we have for any $a \in \mathbf{F}_{2^m}^*$:

$$K(a) - 1 \equiv -C(a, a) \pmod 3.$$

But, when $C(a, a)$ is a nonzero power of 2 it cannot be divisible by 3. We deduce that 3 divides $K(a) - 1$ if and only if $C(a, a) = 0$. We know that $C(a, a) = 0$ if and only if $Tr(a^{1/3}) = 0$ (see [3]).

There is also another point of view, that we develop now. We compute $C(1)$, using (15). For any $h \in \mathbf{F}_{2^m}$:

$$\begin{aligned} C(1) &= \sum_{x \in \mathbf{F}_{2^m}} e(x^3) = \sum_{x \in \mathbf{F}_{2^m}} e\left((x+h)^3\right) \\ &= (-1)^{\mathrm{Tr}(h^3)} C(1, h^4 + h) = 0. \end{aligned}$$

The map $h \mapsto h^4 + h$ is 2-to-1 on $\mathbf{F}_{2^m}$, for odd m. So, we get 2^{m-1} values $C(1, a)$ with $a = h^4 + h$. We have got here all the a such that $C(1, a) = 0$, because it is well known that $C(1, a) = 0$ if and only if $Tr(a) = 0$ (see [2, Theorem 2]).

Now set $a = b^3$ for some b. We have seen that $C(1, b) = 0$ if and only if there is an h such that $h^4 + h + b = 0$. Setting $h = by$ we have the following equivalent equations:

$$h^4 + h + b = 0 \Leftrightarrow b^4y^4 + by + b = 0$$

which is equivalent to

$$bay^4 + by + b = 0 \Leftrightarrow ay^4 + y + 1 = 0.$$

So $a = (y+1)/y^4$, which is by replacing $y = (z+1)^2$:

$$a^2 = \frac{z^2}{(z^4+1)^2} = \left(\frac{z}{z^4+1}\right)^2.$$

Assume now that m is even, $m = 2s$. In this case, we can use Theorem 18 where the three possible values of $K(a) \pmod 3$ are studied. We directly obtain that

$$K(a) - 1 \equiv 0 \pmod 3 \Leftrightarrow C(a,a) = 0$$

(case **(3)** of this theorem). In accordance with Theorem 5, $C(a,a) = 0$ if and only if a is a cube such that $T_2^m(a^{1/3}) \neq 0$, completing the proof. □

7. Conclusion

In this paper, we study some divisibility properties of classical binary Kloosterman sums. However, our main purpose is to point out the interesting (and often surprising) relations which appear between these sums, the cubic sums and the inverse cubic sums. Formula (6) and (7) show clearly these relations, as well as the involvement of these sums in the weight distributions of cosets of the 3-error-correcting BCH-code. Moreover our results lead us to several open problems. It is first the spectrum of $K(a)$ modulo 24. We were able to give it for odd m in [4], but the even case seems more difficult. To obtain, even for specific a, the values of $K(a)$ by means of other exponential sums or of the values $\mu(\epsilon, \lambda)$, using (6) and (7), is a more general and difficult problem.

There is a natural expansion of Theorem 22, since the general problem of the computation of $K(a) - 1$ modulo 3 is not considered. When m is even, Theorem 18 could be used extensively.

References

[1] E.R. Berlekamp, H. Rumsey, G. Solomon, On the solution of algebraic equations over finite fields, Information and Control 12 (5) (1967) 553–564.
[2] L. Carlitz, Explicit evaluation of certain exponential sums, Math. Scand. 44 (1979) 5–16.
[3] P. Charpin, T. Helleseth, V.A. Zinoviev, On cosets of weight 4 of binary BCH codes with minimum distance 8 and exponential sums, Probl. Inf. Trans. 41 (4) (2005) 301–320.
[4] P. Charpin, T. Helleseth, V.A. Zinoviev, The divisibility modulo 24 of Kloosterman sums on GF(2^m), m odd, J. Combin. Theory, Ser. A 114 (2) (2007) 322–338.
[5] P. Charpin, T. Helleseth, V.A. Zinoviev, On cosets of weight 4 of binary primitive BCH codes of length 2^m (m even) with minimum distance 8 and exponential sums, SIAM J. Discrete Math. 23 (1) (2008) 59–78.
[6] P. Charpin, V.A. Zinoviev, On coset weight distributions of the 3-error-correcting BCH-codes, SIAM J. Discrete Math. 10 (1) (1997) 128–145.
[7] J.F. Dillon, Elementary Hadamard difference sets, in: Proc. 6-th S-E Conf. Combinatorics, Graph theory, and Computing, Congress Number XIV, 1975, pp. 237–249.
[8] K. Garaschuk, P. Lisonek, On Kloosterman sums divisible by 3, Des., Codes Cryptogr. 49 (2008) 347–357.
[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] P.V. Kumar, T. Helleseth, R. Calderbank, R. Hammons, Large families of quaternary sequences with low correlation, IEEE Trans. Inform. Theory 42 (2) (1996) 579–592.