Divisibility properties of Kloosterman sums over finite fields of characteristic two

Pascale Charpin
INRIA, Codes
Domaine de Voluceau-Rocquencourt
BP 105 - 78153, Le Chesnay
France
Email: pascale.charpin@inria.fr

Tor Helleseth
The Selmer Center
Department of Informatics
University of Bergen
PB 7800, N-5020 Bergen, Norway
Email: torh@ii.uib.no

Victor Zinoviev
Institute for Problems of Inf. Trans.
Russian Academy of Sciences
Bol'shoi Karetnyi per. 19, GSP-4
Moscow, 101447, Russia
Email: zinov@iitp.ru

***Abstract*— Let $K(a)$ be the so-called classical Kloosterman sums over $\mathbf{F}_{2^m}$, where m is even. In this paper, we compute $K(a)$ modulo 24, completing our previous results for odd m. We extensively study the links between $K(a)$ and other exponential sums, in particular with the cubic sums. We point out (as we did for odd m) that the values $K(a)$ are related with cosets of weight 4 of primitive narrow sense extended BCH codes of length $n = 2^m$ and minimum distance 8.**

Keywords: BCH code, coset weight distribution, Kloosterman sum, cubic sum, inverse cubic sum.

I. Introduction

We denote by $K(a)$, $a \in \mathbf{F}_{2^m}$, the so-called classical binary Kloosterman sums 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 [8], [4], [6], [7]) and on the relations which link the weight distribution of any coset $D^{(4)}$ with the spectrum of three exponential sums, including Kloosterman sums. In [5], 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 treat the even case (m even) and found the exact expression for the number of coset leaders of any coset $D^{(4)}$ [7]. 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 II, includes the definitions and properties which we need for the next sections. Most of them are known. By Lemma 5, we exhibit some relations between $K(a)$ and partial cubic sums which are particularly important in the even case. In Section III, we recall our main result concerning cosets $D^{(4)}$ of B_m [4], [7] (see Theorem 2) and show how we can extend our result for odd m to any m. Section IV is 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 V, 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 5.

In the last section, we give an alternative description of divisibility of $K(a)-1$ by 3, obtained in the recent paper [9].

This paper is an extended abstract, so that several proofs are not given or are shortened.

II. 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 $e(p(x)) = (-1)^{Tr(p(x))}$ where Tr is the absolute trace over $\mathbf{F}_{2^m}$, and $e(a)$ is an additive character of $\mathbf{F}_{2^m}$. For the case of even m, we use also the trace function from $\mathbf{F}_{2^m}$ to its subfield $\mathbf{F}_4$, denoted by $Tr_2^m(x)$, i.e.

$$Tr_2^m(x) \;=\; x + x^4 + x^{4^2} + \cdots + x^{4^{s-1}}, \quad m = 2s.$$

For any set V, $V^* = V \setminus \{0\}$.

A. 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 $Tr(a^3/b^2) = Tr(1)$.

Denote $f_b(x) = x^3 + x + b$, where $b \in \mathbf{F}_{2^m}^*$. Let

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

Lemma 2: [11] Let $n = 2^m$. If m is odd, then

$$\left.\begin{array}{lcl} M_0 & = & (n+1)/3, \\ M_1 & = & (n-2)/2, \\ M_3 & = & (n-2)/6. \end{array}\right\}$$

If m is even, then

$$\left.\begin{array}{lcl} M_0 & = & (n-1)/3, \\ M_1 & = & n/2, \\ M_3 & = & (n-4)/6. \end{array}\right\}$$

B. Some exponential sums

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

Definition 1: The classical Kloosterman sums are:

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

The cubic sums are:

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

The *inverse cubic* sums are:

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

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

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

In fact: $Tr(x^{-1}) = Tr(x^{2^{m-1}-1})$ and $Tr(x^{-3}) = Tr(x^{2^{m-2}-1})$.

The spectrum of the cubic sum $C(a,b)$ was first specified by Carlitz [3]. 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 [3, Theorem 1]. The sums $C(a,0)$ is denoted by $C(a)$.

Theorem 1: 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 $ax^4+x+a=0$.

C. Useful Properties

Lemma 3: [10] For any m

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

Lemma 4: [7] For any $a\in\mathbf{F}_{2^m}^*$ and any m:

$$\begin{aligned} K(a) &= 2\sum_{x\in\mathbf{F}_{2^m},\ Tr(1/x)=0} e(ax) \\ &= -2\sum_{x\in\mathbf{F}_{2^m},\ Tr(1/x)=1} e(ax). \end{aligned}$$

Lemma 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.

Proof: We have first

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

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

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

We use now Lemmas 1 and 2. The equation $x^3+x+c=0$ has a unique solution if and only if $Tr(1/c)\neq Tr(1)$.

Assume first that m is odd. So $Tr(1)=1$ and we know that there are $2^{m-1}-1$ elements $c\in\mathbf{F}_{2^m}^*$ such that $Tr(1/c)=0$. The mapping $x\mapsto x^3+x$ is a permutation on the set of $x\in\mathbf{F}_{2^m}^*$ such that $Tr(1/x)=0$, according to (2).Then, the next equality holds.

$$\begin{aligned} &\{\ x^3+x \mid x\in\mathbf{F}_{2^m}^*,\ Tr(1/x)=0\ \} \\ &\quad = \{\ y\in\mathbf{F}_{2^m}^* \mid Tr(1/y)=0\ \}. \end{aligned}$$

We deduce, using Lemma 4,

$$P(a,a) = \sum_{x,\ Tr(1/x)=0} e(a(x^3+x)) = \sum_{y,\ Tr(1/y)=0} e(ay) = \frac{K(a)}{2}.$$

Now, let m be even so that $Tr(1)=0$ and we know that there are 2^{m-1} elements c such that $Tr(1/c)=1$. In this case $x\mapsto x^3+x$ is a permutation on the set of $x\in\mathbf{F}_{2^m}$ such that $Tr(1/x)=1$. Then, the next equality holds.

$$\begin{aligned} &\{\ x^3+x \mid x\in\mathbf{F}_{2^m},\ Tr(1/x)=1\ \} \\ &\quad = \{\ y\in\mathbf{F}_{2^m} \mid Tr(1/y)=1\ \}. \end{aligned}$$

We deduce

$$\sum_{x,\ Tr(1/x)=1} e(a(x^3+x)) = \sum_{y,\ Tr(1/y)=1} e(ay),$$

and, using (1) and Lemma 4,

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

■

III. The number of solutions to the nonlinear system 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 $\mathbf{F}_{2^m}$:

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

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 (3). Then there are $\varepsilon \in \mathbf{F}_2$ and $\lambda \in \mathbf{F}_{2^m}^*$

$$\varepsilon = Tr\left(\frac{b}{a^3}\right) \quad \text{and} \quad \lambda = \frac{c}{a^5} + \frac{b^2}{a^6} + \frac{b}{a^3} + 1, \tag{4}$$

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

Theorem 2: For $m \geq 5$ the value $\mu(\varepsilon,\lambda)$ is an even integer, given by the following expressions:

- for even m [7]:

$$\begin{aligned} 24\mu(\varepsilon,\lambda) &= 2^m - 8 + 3\cdot G(\lambda,\lambda) + C(\lambda) \\ &+ (-1)^{\varepsilon}\left(2K(\lambda) + 4C(\lambda,\lambda) - 8\right), \end{aligned} \tag{5}$$

- and for odd m [4]:

$$\begin{aligned} 24\mu(\varepsilon,\lambda) &= 2^m - 8 + 3\cdot G(\lambda,\lambda) \\ &+ (-1)^{\varepsilon+1}\left(2K(\lambda) + 2C(\lambda,\lambda) - 8\right)) \end{aligned} \tag{6}$$

  where λ and ε are given by (4).
- Furthermore, when $\lambda = 0$ then $\mu(\varepsilon,0) = 0$ for even and odd m.

Note that in [4], in the corresponding expression for $\mu(\varepsilon,\lambda)$ (see (19) in [4]) the cubic sum was $C(1,\lambda^{1/3})$. For odd m it is easy to see, that $C(a,a) = C(1,b)$ where $a = b^3$. Indeed, since $x \mapsto x^3$ is a permutation on $\mathbf{F}_{2^m}$, we have

$$C(a,a) = \sum_{x\in\mathbf{F}_{2^m}} e(ax^3 + ax) = \sum_{y\in\mathbf{F}_{2^m}} e(y^3 + by) = C(1,b) \tag{7}$$

where $x = y/b$.

We deduce two corollaries from the previous theorem. For both, the case where m is odd was already proved in [5]. We are now able to treat the even case too.

Corollary 1: For any $m \geq 4$, any $\varepsilon \in \mathbf{F}_2$ and any $\lambda \in \mathbf{F}_{2^m}^*$, where $\mathbf{F}_{2^m}$ has order 2^m, the number at the right hand side of the equality (5) (resp.(6)) is a positive integer divisible by 48.

Corollary 2: 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. If λ is a cube then

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

Otherwise, then $m = 2s$ and (8) holds for $m \geq 8$.

Proof: We already proved the case where m is odd in [5, 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 (5) in Theorem 2. Note that the value $K(\lambda)$ is multiple of 4, for any $\lambda \in \mathbf{F}_{2^m}^*$. Moreover, from Theorem 1, $C(\lambda)$ 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 $m \geq 6$. The result is then obtained by using Lemma 3.

When λ is not a cube, the cubic sums $C(\lambda)$ and $C(\lambda,\lambda)$ are congruent to 0 modulo 2^s and the result holds as soon as $s \geq 4$. ∎

Using the previous corollaries, we get also the first congruence linking $K(a)$ to cubic sums for even m.

Corollary 3: Let $m \geq 8$ be any integer and let $\lambda \in \mathbf{F}_{2^m}^*$. Set

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

where $\mu(\varepsilon,\lambda)$ is given by (5) for even m and by (6) for odd m. Then for any $\varepsilon \in \mathbf{F}_2$, we have

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

IV. 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 [5], 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 we are able to prove directly the main congruences for any m (see the next theorem).

Lemma 6: 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: 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 (2),

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

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 (2),

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

∎

Theorem 3: 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: Let m be odd. Then, using Lemma 5 and (1),

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

But the sum above on the right is equal to $B + 1$ where B is divisible by 3 (see Lemma 6). Then

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

which gives the statement.

Now assume that m is even. Using Lemma 5, we get

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

where $P(a,a)$ is equal to $A+2$ where A is divisible by 3 (see Lemma 6). Hence

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

■

The next theorem is our main congruence modulo 24. From now on, we treat the even case only (see [5] for odd m).

Theorem 4: Let $m = 2s$ with $s \geq 3$. Let $a \in \mathbf{F}_{2^m}^*$. Then we have: If $Tr(a) = 0$ then

$$K(a) - C(a,a) \equiv 16 \pmod{24} \tag{9}$$

else

$$K(a) - C(a,a) \equiv 4 \pmod{24}. \tag{10}$$

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

$$K(a) - C(a,a) \equiv 1 \pmod 3. \tag{11}$$

Now, we use the result of Carlitz [3], which is clearly expressed by Theorem 1. 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 3. If $Tr(a) = 0$ 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 $Tr(a) = 1$ 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. ■

V. 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 $C(a,a)$ which do not hold when m is odd. The next theorem (comparing to [5, Theorem 3.]) shows the differences between the even case (m even) and the odd case (m odd).

Lemma 7: Let $r \geq 3$. Then

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

Theorem 5: 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 II-B. Then we have:

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

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

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

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

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

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

Proof: We simply apply Theorem 4. Before, we have to specify the divisibility of $C(a)$. From Theorem 1, we know that $C(a) = (-1)^r 2^r$ with $r = s$ or $r = s+1$. From Lemma 7, we get

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

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

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

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

Using (9) and (10), 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, $K(a) \equiv 0 \pmod 3$.

Now, 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 1). In this case the divisibility of K(a) is directly obtained from Theorem 4. And this is clearly the case where $K(a) \equiv 1 \pmod 3$. ■

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

Theorem 6: Let $m = 2s$ with $m \geq 4$. Then we have for any $a \in \mathbf{F}_{2^m}^*$:

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

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

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

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

and for even s

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

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

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

and for even s

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

Proof: The case $C(a,a) = 0$ is given by Theorem 5, **3)**. Assume that $C(a,a) \in \{2^s, -2^{s+1}\}$. Using Theorem 1, 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 5, **2)**, and Theorem 5,**1)**, respectively. We treat the case $C(a,a) \in \{-2^s, 2^{s+1}\}$ by the same way. ■

VI. Another divisibility modulo 3

In this section we study the divisibility by 3 of $K(a)-1$. In [10] it has been proved that for odd m and any a

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

In [5], we specified $K(a)-1$ modulo 3, but for odd m only. Another expression is proposed by [9], also for odd m. For even m and any a we have from [10] 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 result of [4] and also completely solve the case of even m, by proving the following theorem.

Theorem 7: 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
$$a=b^3 \quad \text{for some } b \text{ such that } \quad T_2^{2s}(b)\neq 0.$$
- In both cases $K(a)-1$ is divisible by 3 if and only if $C(a,a)=0$.

Proof: Let m be odd, so that $x \mapsto ax^3$ is a permutation which means notably that $C(a)=0$, for any $a \in \mathbf{F}_{2^m}^*$. We start from the congruences given by Theorem 3. For any $a \in \mathbf{F}_{2^m}^*$

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

If $C(a,a)\neq 0$, it is never 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 [4]).

There is also the other point of view, that we develop now. Clearly, we have for any $h \in \mathbf{F}_{2^m}$:

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

Since the map $h \mapsto h^4+h$ is 2-to-1, we then get 2^{m-1} values $C(1,a)$ with $a=h^4+h$. Note that, for any a, $h+1$ and h are the solutions of $a=h^4+h$. Since

$$Tr((h+1)^3) = Tr(h^3+h^2+h+1) = Tr(h^3)+1$$

then either h or $h+1$ has trace zero. Hence we have got here all the a such that $C(1,a)=0$. Now come back to $a=b^3$ with $C(1,b)=0$. This holds if and only if there is h such that $h^4+h+b=0$. Setting $h=by$ we get

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

which is equivalent to

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

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

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

Let $m=2s$. In this case, we can use Theorem 5, **3)**, where the case

$$K(a) \ - \ 1 \ \equiv \ 0 \quad (\text{mod } 3),$$

is treated. ∎

Remark 1: There is a natural expansion of the previous theorem, since the general problem of the computation of $K(a)-1$ modulo 3 is not considered. When m is even, Theorem 5 could be used extensively.

VII. 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 (5) and (6) 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 [5], 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 $\mu(\varepsilon,\lambda)$, using (5) and (6), is a more general and difficult problem.

References

[1] E.R. Berlekamp, H. Rumsey & G. Solomon, "On the solution of algebraic equations over finite fields", *Information and Control*, vol. 12, no. 5, pp. 553-564, Oct. 1967.

[2] L. Carlitz, "Kloosterman sums and finite field extensions", *Acta Arithmetica*, vol. XVI, no. 2, pp. 179-193, 1969.

[3] L. Carlitz, "Explicit evaluation of certain exponential sums", *Math. Scand.*, vol. 44, pp. 5-16, 1979.

[4] P. Charpin, T. Helleseth & V.A. Zinoviev, "On cosets of weight 4 of binary BCH codes with minimum distance 8 and exponential sums", *Problems of Information Transmission*, vol. 41, no. 4, pp. 301-320, 2005.

[5] P. Charpin, T. Helleseth, & V.A. Zinoviev, "The divisibility modulo 24 of Kloosterman sums on GF(2^m), m odd". *Journal of Combinatorial Theory, Series A*, vol. 114, Issue 2, pp. 322-338, 2007.

[6] P. Charpin, T. Helleseth & V.A. Zinoviev, "The Coset Distribution of the Triple-Error-Correcting Binary Primitive BCH Codes", IEEE Trans. Inform. Theory, vol. 52, No. 4, pp. 1727-1732, 2006.

[7] 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". *SIAM J. of Discrete Math.*, 2007, submitted.

[8] P. Charpin & V.A. Zinoviev, "On coset weight distributions of the 3-error-correcting BCH-codes", *SIAM J. Discrete Math.*, vol. 10, no. 1, pp. 128-145, February 1997.

[9] K. Garaschuk & P. Lisonek, "On Kloosterman sums divisible by 3", *Designs, Codes and Cryptography*, to appear.

[10] T. Helleseth & V.A. Zinoviev, "On Z_4-Linear Goethals Codes and Kloosterman Sums", *Designs, Codes and Cryptography*, vol. 17, no. 1-3, pp. 246-262, 1999.

[11] P.V. Kumar, T. Helleseth, R. Calderbank & R. Hammons, "Large Families of Quaternary Sequences with Low Correlation", *IEEE Trans. Inform. Theory*, vol. 42, No. 2, pp. 579-592, March 1996.