Finite Fields and Their Applications 15 (2009) 174–184

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

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

Marko Moisio

Department of Mathematics and Statistics, Faculty of Technology, University of Vaasa, PO Box 700, FIN-65101, Finland

ARTICLE INFO

Article history:
Received 27 July 2008
Revised 5 November 2008
Available online 11 December 2008
Communicated by Gary L. Mullen

Keywords:
Kloosterman sum
Divisibility
Elliptic curve
Exponential sum

ABSTRACT

In a recent work by Charpin, Helleseth, and Zinoviev Kloosterman sums $K(a)$ over a finite field $\mathbb{F}_{2^m}$ were evaluated modulo 24 in the case m odd, and the number of those a giving the same value for $K(a)$ modulo 24 was given. In this paper the same is done in the case m even. The key techniques used in this paper are different from those used in the aforementioned work. In particular, we exploit recent results on the number of irreducible polynomials with prescribed coefficients.

1. Introduction

Let $\mathbb{F}_{2^m}$ denote the finite field of 2^m elements, $m > 2$, and let $a \in \mathbb{F}_{2^m}$, $a \neq 0$. Kloosterman sums $K(a)$ over $\mathbb{F}_{2^m}$ are widely studied for a long time for their own sake as interesting mathematical objects as well as for their connection to coding theory, most notably to the weight distribution of the Melas codes (see e.g. [2,6,8] and the bibliography in them).

The value set of $K(a)$ was obtained by Lachaud and Wolfmann [6], and moreover, they gave the number of preimages of a specific value in terms of Kronecker class numbers. However, very little is known of the value $K(a)$ for a specific element a. A recent result towards to the solution of this very difficult but important problem was obtained by Charpin, Helleseth, and Zinoviev [1] who gave congruences modulo 24 for $K(a)$ in the case m odd. In this paper congruences modulo 24 are derived in the case m even. The tools used in this paper are different from those used in [1]: there $K(a)$ is linked to the number of words in a coset of weight 4 in BCH-code with minimum distance 8, and cubic exponential sums evaluated by Carlitz, but in this paper $K(a)$ is linked to the number of irreducible cubic polynomials with prescribed norm and trace, and to the number of solutions of $x^4 + x^3 = a$ in $\mathbb{F}_{2^m}$. In the calculation of the number of those elements $a \in \mathbb{F}_q^*$ which yield the

E-mail address: mamo@uwasa.fi.

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2008.11.001

same value for $K(a)$ modulo 24 explicit evaluations of certain exponential sums are also needed, and we shall see that the value distribution of $K(a)$ modulo 24 depends on the residue class of m modulo 24.

The rest of the paper is organized as follows. In Section 2 notations are fixed and some previous divisibility results needed are recalled. In Section 3 congruences modulo 3 for $K(a^4+a^3)$ are obtained by considering a family of elliptic curves related to the number of irreducible cubic polynomials with prescribed trace and norm. In Section 4 the number of solutions of $x^{2^k}+x^{2^k-1}=a$ in $\mathbb{F}_{2^m}$ is calculated. In Section 5, $K(a)$ is evaluated modulo 24 in the case m even (Theorem 11), and finally, in Section 6, the number of non-zero elements $a \in \mathbb{F}_{2^m}$ which yield the same value for $K(a)$ modulo 24 is given (Theorems 15 and 18).

2. Preliminaries

In this section we fix some notations and recall some previous divisibility results of Kloosterman sums needed in the sequel.

Let $m > 2$ be an integer and let s be a positive factor of m. Let $q = 2^m$ and let $\mathbb{F}_q$ denote the finite field of q elements and let $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. Let Tr_s denote the trace function from $\mathbb{F}_q$ onto $\mathbb{F}_{2^s}$ i.e.

$$\mathrm{Tr}_s(x) = x + x^{2^s} + x^{2^{2s}} + \cdots + x^{2^{(\frac{m}{s}-1)s}} \quad \forall x \in \mathbb{F}_q.$$

Moreover, we use the notation Tr instead of Tr_1.

Let $a \in \mathbb{F}_q$ and let χ be the canonical additive character of $\mathbb{F}_q$ i.e. $\chi(x) = (-1)^{\mathrm{Tr}(x)}$ for all $x \in \mathbb{F}_q$. We shall use frequently the following well-known result, the orthogonality of characters:

$$\sum_{x \in \mathbb{F}_q} \chi(ax) = \begin{cases} q & \text{if } a = 0, \\ 0 & \text{if } a \neq 0. \end{cases}$$

Let $K(a)$ denote the Kloosterman sum defined by

$$K(a) = \sum_{x \in \mathbb{F}_q^*} \chi\left(x + ax^{-1}\right).$$

We have the following result by Helleseth and Zinoviev.

Proposition 1. *(See [4].) Let $a \in \mathbb{F}_q^*$. Then*

$$K(a) \equiv \begin{cases} 3 \pmod 8 & \text{if } \mathrm{Tr}(a) = 1, \\ -1 \pmod 8 & \text{if } \mathrm{Tr}(a) = 0. \end{cases}$$

Moreover, we have the following result from [9].

Proposition 2. *Let $a \in \mathbb{F}_q^*$. Then $K(a) \equiv 0 \pmod 3$ if and only if one of the following condition holds*

(1) *m is odd and $\mathrm{Tr}(\sqrt[3]{a}) = 0$,*
(2) *m is even, $a = b^3$ for some $b \in \mathbb{F}_q$, and $\mathrm{Tr}_2(b) \neq 0$.*

Remark 3. In the case m odd Proposition 2 follows also from Theorem 3 in [1].

3. Kloosterman sums and irreducible cubic polynomials

Let $a, b \in \mathbb{F}_q^*$, and let $P_3(a,b)$ denote the number of irreducible polynomials $x^3 + ax^2 + dx + b \in \mathbb{F}_q[x]$. Let $\mathcal{X}$ be the projective elliptic curve over $\mathbb{F}_q$ defined by

$$\mathcal{X} : y^2 + cy + xy = x^3,$$

where $c = b/a^3$, and let $|\mathcal{X}(\mathbb{F}_q)|$ denote the number of rational points on $\mathcal{X}$.

We have the following special case of [9, Theorem 7.3]

Proposition 4.

$$P_3(a,b) = \frac{1}{3}\left(\left|\mathcal{X}(\mathbb{F}_q)\right| - \epsilon\right),$$

where ϵ equals 1 or 0 depending on whether $c = 1$ or $c \neq 1$.

By using Proposition 4 we are able to prove the main result of this section:

Theorem 5. *Let $c \in \mathbb{F}_q^*$, $c \neq 1$. Then*

$$K(c^4 + c^3) \equiv \begin{cases} 1 \pmod 3 & \text{if } m \text{ is even and } \mathrm{Tr}(c) = 0, \\ -1 \pmod 3 & \text{if } m \text{ is even and } \mathrm{Tr}(c) = 1, \\ 0 \pmod 3 & \text{if } m \text{ is odd.} \end{cases}$$

Proof. By Proposition 4

$$3P_3(1,c) = \left|\mathcal{X}(\mathbb{F}_q)\right|$$

where $\mathcal{X} : y^2 + cy + xy = x^3$. Write the equation of $\mathcal{X}$ in the form

$$y^2 + (x+c)y = x^3.$$

For a fixed $x \neq c$ substitute $y \mapsto (x+c)y$ to get the equation in the form

$$y^2 + y = x^3/(x+c)^2.$$

Hence, by the orthogonality of characters, the number of solutions (x,y) with $x \neq c$ in $\mathbb{F}_q^2$ of $y^2 + cy + xy = x^3$ is equal to

$$\begin{aligned} N \;&:=\; \sum_{x \in \mathbb{F}_q,\, x \neq c} \left(1 + \chi\left(\frac{x^3}{(x+c)^2}\right)\right) \\ &\overset{x \mapsto x+c}{=} q - 1 + \sum_{x \in \mathbb{F}_q^*} \chi\left(\frac{(x+c)^3}{x^2}\right) \\ &= q - 1 + \sum_{x \in \mathbb{F}_q^*} \chi\left(x + c + c^2x^{-1} + c^3x^{-2}\right) \\ &= q - 1 + \chi(c) \sum_{x \in \mathbb{F}_q^*} \chi(x)\chi\left(c^2x^{-1}\right)\chi\left(c^3x^{-2}\right). \end{aligned}$$

Since $\mathrm{Tr}(z) = \mathrm{Tr}(z^2)$ for all $z \in \mathbb{F}_q$, we now get

$$N = q - 1 + \chi(c) \sum_{x \in \mathbb{F}_q^*} \chi\left(x^2 + c^4 x^{-2} + c^3 x^{-2}\right) = q - 1 + \chi(c) K\left(c^4 + c^3\right),$$

where the last equation follows by noting that $x \mapsto x^2$ is a permutation of $\mathbb{F}_q$.

Since equation $y^2 + cy + xy = x^3$ has exactly one solution with $x = c$, and since $\mathcal{X}$ has exactly one point at infinity, we now get

$$3P(1,c) = \left|\mathcal{X}(\mathbb{F}_q)\right| = q + 1 + \chi(c) K\left(c^4 + c^3\right),$$

and consequently $\chi(c) K(c^4 + c^3) \equiv -q - 1 \pmod 3$. Since $q \equiv (-1)^m \pmod 3$, we get

$$\chi(c) K(c^4 + c^3) \equiv \begin{cases} 1 \pmod 3 & \text{if } m \text{ is even}, \\ 0 \pmod 3 & \text{if } m \text{ is odd}. \end{cases}$$

This completes the proof, since $\chi(c) = 1, -1$ depending on whether $\mathrm{Tr}(c) = 0, 1$. $\square$

Remark 6. Theorem 5 is also proved in [4] by using different methods.

Remark 7. If we can prove in the case m even that all such elements a in $\mathbb{F}_q^*$, which do not satisfy the condition in Proposition 2, can be written in the form $a = c^4 + c^3$, then Proposition 2 and Theorem 5 give the divisibility modulo 3 of $K(a)$ for all $a \in \mathbb{F}_q^*$. We shall see in the next section that this indeed is the case.

4. The equation $x^{2^k} + x^{2^k - 1} = a$

In this section we shall prove the following

Theorem 8. *Let k be a positive integer and let $a \in \mathbb{F}_q^*$. The number $N(a)$ of solutions of*

$$x^{2^k} + x^{2^k - 1} = a \tag{1}$$

is given by

$$N(a) = \begin{cases} 1 & \text{if } a \neq b^{2^k - 1} \text{ for all } b \in \mathbb{F}_q, \\ 2^s & \text{if } a = b^{2^k - 1} \text{ for some } b \in \mathbb{F}_q, \text{ and } \mathrm{Tr}_s(b) = 0, \\ 0 & \text{if } a = b^{2^k - 1} \text{ for some } b \in \mathbb{F}_q, \text{ and } \mathrm{Tr}_s(b) \neq 0, \end{cases}$$

where $s = \gcd(k, m)$.

Proof. Substitute $x \mapsto x^{-1}$ to (1) and then multiply both sides by x^{2^k} to get an equivalent equation

$$1 + x = a x^{2^k}.$$

Now, by the orthogonality of characters, we get

$$qN(a) = \sum_{c \in \mathbb{F}_q} \sum_{x \in \mathbb{F}_q} \chi\left(c\left(1 + x + a x^{2^k}\right)\right) = q + \sum_{c \in \mathbb{F}_q^*} \chi(c) \sum_{x \in \mathbb{F}_q} \chi(cx) \chi\left(c a x^{2^k}\right).$$

Since $\chi(z^{2^k}) = \chi(z)$ for all $z \in \mathbb{F}_q$, we obtain

$$qN(a) = q + \sum_{c \in \mathbb{F}_q^*} \chi(c) \sum_{x \in \mathbb{F}_q} \chi\big((c^{2^k} + ca)x^{2^k}\big).$$

Since $x \mapsto x^{2^k}$ is a permutation of $\mathbb{F}_q$, the orthogonality of characters implies that the inner sum

$$\sum_{x \in \mathbb{F}_q} \chi\big((c^{2^k} + ca)x^{2^k}\big) = \begin{cases} 0 & \text{if } c^{2^k-1} \neq a, \\ q & \text{if } c^{2^k-1} = a. \end{cases}$$

Hence, if $c^{2^k-1} = a$ is not solvable, then $N(a) = 1$. On the other hand, $c^{2^k-1} = a$ is solvable if and only if a is in $\langle \gamma^{2^s-1} \rangle$ since $\gcd(2^k - 1, 2^m - 1) = 2^s - 1$. Moreover, if b is one solution, then all the solutions are $b\alpha$ where α runs over $\mathbb{F}_{2^s}^*$. Hence, if $a = b^{2^k-1}$ for some $b \in \mathbb{F}_q^*$, then

$$qN(a) = q + q \sum_{\alpha \in \mathbb{F}_{2^s}^*} \chi(b\alpha) = \begin{cases} q2^s & \text{if } \mathrm{Tr}_s(b) = 0, \\ 0 & \text{if } \mathrm{Tr}_s(b) \neq 0, \end{cases}$$

and therefore, in this case,

$$N(a) = \begin{cases} 2^s & \text{if } \mathrm{Tr}_s(b) = 0, \\ 0 & \text{if } \mathrm{Tr}_s(b) \neq 0, \end{cases}$$

completing the proof. □

Corollary 9. *Assume* $\gcd(k, m) = 1$. *Then*

$$N(a) = \begin{cases} 2 & \textit{if } \mathrm{Tr}(a^{\frac{1}{2^k-1}}) = 0, \\ 0 & \textit{otherwise.} \end{cases}$$

Remark 10. In the case m odd Corollary 9 was also proved in [3] by using different methods. Moreover, Corollary 9, Theorem 5 and Proposition 2 imply that in the case m odd $K(a)$ is divisible by 3 if and only if $a = c^4 + c^3$ for some $c \in \mathbb{F}_q^*$. This is proved in [3] by using Theorem 3 in [1].

5. The evaluation of $K(a)$ modulo 24, m even

We are now able to evaluate $K(a)$ modulo 24:

Theorem 11. *Let* $a \in \mathbb{F}_q^*$.

(1) *Assume* $a = b^3$ *for some* $b \in \mathbb{F}_q$ *with* $\mathrm{Tr}_2(b) \neq 0$. *Then,* $a \neq c^4 + c^3$ *for all* $c \in \mathbb{F}_q^*$, *and*

$$K(a) \equiv \begin{cases} 15 \pmod{24} & \textit{if } \mathrm{Tr}(a) = 0, \\ 3 \pmod{24} & \textit{if } \mathrm{Tr}(a) = 1. \end{cases}$$

(2) *Otherwise,* $a = c^4 + c^3$ *for some* $c \in \mathbb{F}_q^*$, *and*

$$K(a) \equiv \begin{cases} 7 \pmod{24} & \textit{if } \mathrm{Tr}(c) = 0 \textit{ and } \mathrm{Tr}(c^3) = 0, \\ 19 \pmod{24} & \textit{if } \mathrm{Tr}(c) = 0 \textit{ and } \mathrm{Tr}(c^3) = 1, \\ 11 \pmod{24} & \textit{if } \mathrm{Tr}(c) = 1 \textit{ and } \mathrm{Tr}(c^3) = 0, \\ 23 \pmod{24} & \textit{if } \mathrm{Tr}(c) = 1 \textit{ and } \mathrm{Tr}(c^3) = 1. \end{cases}$$

Proof. If $a = b^3$ for some $b \in \mathbb{F}_q$ and $\mathrm{Tr}_2(b) = 0$ or $a \neq b^3$ for all $b \in \mathbb{F}_q$, then $a = c^4 + c^3$ for some $c \in \mathbb{F}_q^*$ by Theorem 8 ($k = 2$). Now, by Theorem 5,

$$K(a) \equiv \begin{cases} 1 \pmod 3 & \text{if } \mathrm{Tr}(c) = 0, \\ -1 \pmod 3 & \text{if } \mathrm{Tr}(c) = 1. \end{cases}$$

These congruences and the congruences in Proposition 1 imply

$$K(a) \equiv \begin{cases} 7 \pmod{24} & \text{if } \mathrm{Tr}(a) = 0 \text{ and } \mathrm{Tr}(c) = 0, \\ 23 \pmod{24} & \text{if } \mathrm{Tr}(a) = 0 \text{ and } \mathrm{Tr}(c) = 1, \\ 19 \pmod{24} & \text{if } \mathrm{Tr}(a) = 1 \text{ and } \mathrm{Tr}(c) = 0, \\ 11 \pmod{24} & \text{if } \mathrm{Tr}(a) = 1 \text{ and } \mathrm{Tr}(c) = 1. \end{cases}$$

Since $\mathrm{Tr}(a) = \mathrm{Tr}(c^4) + \mathrm{Tr}(c^3) = \mathrm{Tr}(c) + \mathrm{Tr}(c^3)$, the proof is complete in this case.

In the remaining case we have $a \neq c^4 + c^3$ for all $c \in \mathbb{F}_q^*$, by Theorem 8, and the congruences in Propositions 1 and 2 complete the proof. □

6. The value distribution of $K(a)$ modulo 24, m even

Assume that m is even, and let $a \in \mathbb{F}_q^*$. In this section we shall give the cardinality of the preimage of the remainder $K(a) \bmod 24$ under the map $y \mapsto (K(y) \bmod 24)$ defined on $\mathbb{F}_q^*$. By Theorem 11 it is natural to split the consideration according to whether a can, or can not, be represented in the form $a = c^4 + c^3$ for some $c \in \mathbb{F}_q^*$.

We shall need the following explicit result on exponential sums.

Lemma 12.

$$\sum_{x \in \mathbb{F}_q} \chi\left(x^3\right) = -(-1)^{\frac{m}{2}} 2\sqrt{q},$$

$$\sum_{x \in \mathbb{F}_q} \chi\left(x^9\right) = \begin{cases} -(-1)^{\frac{m}{2}} 2\sqrt{q} & \text{if } m \equiv \pm 1 \pmod 3, \\ -(-1)^{\frac{m}{2}} 8\sqrt{q} & \text{if } m \equiv 0 \pmod 3, \end{cases}$$

$$\sum_{x \in \mathbb{F}_q} \chi\left(x^3 + x\right) = \begin{cases} -2\sqrt{q} & \text{if } m \equiv 0 \pmod 8, \\ 0 & \text{if } m \equiv 2, 6 \pmod 8, \\ 2\sqrt{q} & \text{if } m \equiv 4 \pmod 8, \end{cases}$$

$$\sum_{x \in \mathbb{F}_q} \chi\left(x^9 + x^3\right) = \begin{cases} -8\sqrt{q} & \text{if } m \equiv 0 \pmod 8, \\ 2\sqrt{q} & \text{if } m \equiv 2, 6 \pmod 8, \\ 4\sqrt{q} & \text{if } m \equiv 4 \pmod 8. \end{cases}$$

Proof. Let $S(f) = \sum_{x \in \mathbb{F}_q} \chi(f(x))$. If $f(x) = x^3$, or $f(x) = x^9$ and $m \equiv 0 \pmod 3$, the result is well known (see e.g [7,11]). If $m \equiv \pm 1 \pmod 3$ then $\gcd(9, q-1) = 3$, and therefore $S(x^9) = S(x^3)$. If $f(x) = x^3 + x$ or $f(x) = x^9 + x^3$ we refer to [10, p. 191] and [5, Example 5.7], respectively. □

6.1. *Case $a = c^4 + c^3$ for some $c \in \mathbb{F}_q^*$*

Let γ be a primitive element of $\mathbb{F}_q$. Let $\epsilon, \delta \in \mathbb{F}_2$, and let

$$C(\epsilon, \delta) = \left\{ c \in \mathbb{F}_q^* \setminus \{1\} \,\middle|\, \mathrm{Tr}(c) = \epsilon,\ \mathrm{Tr}\left(c^3\right) = \delta \right\}.$$

Consider the function f on $C(\epsilon,\delta)$ defined by the polynomial $f(x)=x^4+x^3$. Let $N(\epsilon,\delta)$ denote the number of elements c in $C(\epsilon,\delta)$ satisfying $f(c)\in\langle\gamma^3\rangle$.

Lemma 13. *The value of $K(f(c))$ modulo 24 corresponding to the pair $(\mathrm{Tr}(c),\mathrm{Tr}(c^3))=(\epsilon,\delta)$ in Theorem 11 is attained exactly*

$$\#C(\epsilon,\delta)-\tfrac{3}{4}N(\epsilon,\delta)$$

times as c varies over $C(\epsilon,\delta)$. Moreover,

$$N(\epsilon,\delta)=\#\left\{i=1,\dots,\frac{q-1}{3}-1\;\middle|\;\mathrm{Tr}\big(\gamma^{3i}\big)=\epsilon,\ \mathrm{Tr}\big(\gamma^{9i}\big)=\delta\right\}.$$

Proof. Let a be an element in the image of f. Assume $a\in\langle\gamma^3\rangle$. Now, by Theorem 8, there are exactly four elements $c\in\mathbb{F}_q^*$ such that $f(c)=a$. Each such c must belong to $C(\epsilon,\delta)$, for otherwise $\mathrm{Tr}(c)\neq\epsilon$ or $\mathrm{Tr}(c^3)\neq\delta$ leading to a different value $K(a)$ mod 24, by Theorem 11.

If $a\notin\langle\gamma^3\rangle$, then by Theorem 8, a has exactly one preimage under f and therefore $K(a)$ mod 24 is attained exactly $\frac{1}{4}N(\epsilon,\delta)+N'(\epsilon,\delta)$ times, where $N'(\epsilon,\delta)$ is the number of elements c in $C(\epsilon,\delta)$ satisfying $f(c)\notin\langle\gamma^3\rangle$. But $N'(\epsilon,\delta)=\#C(\epsilon,\delta)-N(\epsilon,\delta)$, which proves the first part of the lemma.

To prove the claimed expression for $N(\epsilon,\delta)$, we note that $a=c^3(c+1)\in\langle\gamma^3\rangle$ if and only if $c+1\in\langle\gamma^3\rangle$ if and only if $c=\gamma^{3i}+1$ for some $i=1,\dots,(q-1)/3-1$. If $c=\gamma^{3i}+1$, then $c^3=\gamma^{9i}+\gamma^{6i}+\gamma^{3i}+1$, and consequently

$$\mathrm{Tr}(c)=\mathrm{Tr}\big(\gamma^{3i}\big)+\mathrm{Tr}(1)=\mathrm{Tr}\big(\gamma^{3i}\big)$$

and

$$\mathrm{Tr}\big(c^3\big)=\mathrm{Tr}\big(\gamma^{9i}\big)+\mathrm{Tr}\big(\big(\gamma^{3i}\big)^2\big)+\mathrm{Tr}\big(\gamma^{3i}\big)+\mathrm{Tr}(1)=\mathrm{Tr}\big(\gamma^{9i}\big).$$

Hence, the number $N(\epsilon,\delta)$ of elements c in $C(\epsilon,\delta)$ satisfying $f(c)\in\langle\gamma^3\rangle$ is given by

$$N(\epsilon,\delta)=\left\{i=1,\dots,\frac{q-1}{3}-1\;\middle|\;\mathrm{Tr}\big(\gamma^{3i}\big)=\epsilon,\ \mathrm{Tr}\big(\gamma^{9i}\big)=\delta\right\},$$

which completes the proof. □

Next we shall find exponential sum expressions for the numbers $N(\epsilon,\delta)$ and $\#C(\epsilon,\delta)$.

Lemma 14. *We have*

$$12N(\epsilon,\delta)=q+(-1)^{\delta}\sum_{x\in\mathbb{F}_q}\chi\big(x^9\big)+(-1)^{\epsilon}\sum_{x\in\mathbb{F}_q}\chi\big(x^3\big)+(-1)^{\epsilon+\delta}\sum_{x\in\mathbb{F}_q}\chi\big(x^9+x^3\big)-4h,$$

and

$$4\cdot\#C(\epsilon,\delta)=q+(-1)^{\delta}\sum_{x\in\mathbb{F}_q}\chi\big(x^3\big)+(-1)^{\epsilon+\delta}\sum_{x\in\mathbb{F}_q}\chi\big(x^3+x\big)-2h,$$

where $h=4$ if $\epsilon=\delta=0$, and otherwise $h=0$.

Proof. Let us first calculate $N(\epsilon,\delta)$. Let $z\in\mathbb{F}_q$ satisfying $\mathrm{Tr}(z)=1$ and let ψ be the canonical additive character of $\mathbb{F}_2$. By the orthogonality of characters

$$\begin{aligned}
4N(\epsilon,\delta) &= \sum_{i=1}^{\frac{q-1}{3}-1}\Big(\sum_{u\in\mathbb{F}_2}\psi\big(\mathrm{Tr}\big(\gamma^{3i}+z\epsilon\big)u\big)\Big)\Big(\sum_{v\in\mathbb{F}_2}\psi\big(\mathrm{Tr}\big(\gamma^{9i}+z\delta\big)v\big)\Big)\\
&= \sum_{i=1}^{\frac{q-1}{3}-1}\big(1+(-1)^{\epsilon}\chi\big(\gamma^{3i}\big)\big)\big(1+(-1)^{\delta}\chi\big(\gamma^{9i}\big)\big)\\
&= \sum_{i=1}^{\frac{q-1}{3}-1}\big(1+(-1)^{\delta}\chi\big(\gamma^{9i}\big)+(-1)^{\epsilon}\chi\big(\gamma^{3i}\big)+(-1)^{\epsilon+\delta}\chi\big(\gamma^{9i}+\gamma^{3i}\big)\big)\\
&= \sum_{i=0}^{\frac{q-1}{3}-1}\big(1+(-1)^{\delta}\chi\big(\gamma^{9i}\big)+(-1)^{\epsilon}\chi\big(\gamma^{3i}\big)+(-1)^{\epsilon+\delta}\chi\big(\gamma^{9i}+\gamma^{3i}\big)\big)-h,
\end{aligned}$$

where $h=1+(-1)^{\delta}+(-1)^{\epsilon}+(-1)^{\epsilon+\delta}$. Since the values of γ^{3i} and γ^{9i} depend only on the residue class modulo $(q-1)/3$ of i, we now get

$$\begin{aligned}
4N(\epsilon,\delta)+h &= \frac{1}{3}\sum_{x\in\mathbb{F}_q^*}\big(1+(-1)^{\delta}\chi\big(x^9\big)+(-1)^{\epsilon}\chi\big(x^3\big)+(-1)^{\epsilon+\delta}\chi\big(x^9+x^3\big)\big)\\
&= \frac{1}{3}\sum_{x\in\mathbb{F}_q}\big(1+(-1)^{\delta}\chi\big(x^9\big)+(-1)^{\epsilon}\chi\big(x^3\big)+(-1)^{\epsilon+\delta}\chi\big(x^9+x^3\big)\big)-\tfrac{h}{3},
\end{aligned}$$

from which the claimed formula for $N(\epsilon,\delta)$ follows.

By the orthogonality of characters we also get

$$\begin{aligned}
4\cdot\#C(\epsilon,\delta) &= \sum_{i=1}^{q-2}\Big(\sum_{u\in\mathbb{F}_2}\psi\big(\mathrm{Tr}\big(\gamma^{i}+z\epsilon\big)u\big)\Big)\Big(\sum_{v\in\mathbb{F}_2}\psi\big(\mathrm{Tr}\big(\gamma^{3i}+z\delta\big)v\big)\Big)\\
&= \sum_{i=1}^{q-2}\big(1+(-1)^{\delta}\chi\big(\gamma^{3i}\big)+(-1)^{\epsilon}\chi\big(\gamma^{i}\big)+(-1)^{\epsilon+\delta}\chi\big(\gamma^{3i}+\gamma^{i}\big)\big)\\
&= \sum_{x\in\mathbb{F}_q}\big(1+(-1)^{\delta}\chi\big(x^3\big)+(-1)^{\epsilon}\chi(x)+(-1)^{\epsilon+\delta}\chi\big(x^3+x\big)\big)-2h\\
&= q+(-1)^{\delta}\sum_{x\in\mathbb{F}_q}\chi\big(x^3\big)+(-1)^{\epsilon+\delta}\sum_{x\in\mathbb{F}_q}\chi\big(x^3+x\big)-2h,
\end{aligned}$$

since $\sum_{x\in\mathbb{F}_q}\chi(x)=0$. The proof is now complete. □

Theorem 15. *Let $k \in \{7, 19, 11, 23\}$. The number $T(k)$ of elements a in $\mathbb{F}_q^*$ for which $K(a) \equiv k \pmod{24}$ is given by*

m mod 24	$T(7) - 3 \cdot 2^{m-4}$	$T(19) - 3 \cdot 2^{m-4}$	$T(11) - 3 \cdot 2^{m-4}$	$T(23) - 3 \cdot 2^{m-4}$
0	$2^{\frac{m}{2}-3} - 1$	$2^{\frac{m}{2}-3}$	$-2^{\frac{m}{2}-3}$	$-2^{\frac{m}{2}-3}$
± 6	$-2^{\frac{m}{2}-2} - 1$	0	$2^{\frac{m}{2}-2}$	0
12	$3 \cdot 2^{\frac{m}{2}-3} - 1$	$-2^{\frac{m}{2}-3}$	$-3 \cdot 2^{\frac{m}{2}-3}$	$2^{\frac{m}{2}-3}$
± 8	$-2^{\frac{m}{2}-2} - 1$	$2^{\frac{m}{2}-1}$	$-2^{\frac{m}{2}-1}$	$2^{\frac{m}{2}-2}$
$\pm 2, \pm 10$	$2^{\frac{m}{2}-3} - 1$	$-3 \cdot 2^{\frac{m}{2}-3}$	$5 \cdot 2^{\frac{m}{2}-3}$	$-3 \cdot 2^{\frac{m}{2}-3}$
± 4	-1	$2^{\frac{m}{2}-2}$	$-3 \cdot 2^{\frac{m}{2}-2}$	$2^{\frac{m}{2}-1}$

Proof. Combine Lemmas 14 and 12 to get the following tables for $\frac{3}{4}N(\epsilon, \delta)$ and $\#C(\epsilon, \delta)$:

m mod 24	$\frac{3}{4}N(0,0) - 2^{m-4}$	$\frac{3}{4}N(0,1) - 2^{m-4}$	$\frac{3}{4}N(1,0) - 2^{m-4}$	$\frac{3}{4}N(1,1) - 2^{m-4}$
0	$-9 \cdot 2^{\frac{m}{2}-3} - 1$	$7 \cdot 2^{\frac{m}{2}-3}$	$2^{\frac{m}{2}-3}$	$2^{\frac{m}{2}-3}$
± 6	$3 \cdot 2^{\frac{m}{2}-2} - 1$	$-2^{\frac{m}{2}-1}$	$2^{\frac{m}{2}-2}$	$-2^{\frac{m}{2}-1}$
12	$-3 \cdot 2^{\frac{m}{2}-3} - 1$	$2^{\frac{m}{2}-3}$	$-5 \cdot 2^{\frac{m}{2}-3}$	$7 \cdot 2^{\frac{m}{2}-3}$
± 8	$-3 \cdot 2^{\frac{m}{2}-2} - 1$	$2^{\frac{m}{2}-1}$	$2^{\frac{m}{2}-1}$	$-2^{\frac{m}{2}-2}$
$\pm 2, \pm 10$	$3 \cdot 2^{\frac{m}{2}-3} - 1$	$-2^{\frac{m}{2}-3}$	$-2^{\frac{m}{2}-3}$	$-2^{\frac{m}{2}-3}$
± 4	-1	$-2^{\frac{m}{2}-2}$	$-2^{\frac{m}{2}-2}$	$2^{\frac{m}{2}-1}$

m mod 8	$\#C(0,0) - 2^{m-2}$	$\#C(0,1) - 2^{m-2}$	$\#C(1,0) - 2^{m-2}$	$\#C(1,1) - 2^{m-2}$
0	$-2^{\frac{m}{2}} - 2$	$2^{\frac{m}{2}}$	0	0
± 2	$2^{\frac{m}{2}-1} - 2$	$-2^{\frac{m}{2}-1}$	$2^{\frac{m}{2}-1}$	$-2^{\frac{m}{2}-1}$
4	-2	0	$-2^{\frac{m}{2}}$	$2^{\frac{m}{2}}$

The definitions of ϵ and δ together with Lemma 13 and Theorem 11 now completes the proof. □

Example 16. Let $m = 6$. By [6] we know that the value set of $K(a)$ is $S := \{-13, -9, -5, -1, 3, 7, 11, 15\}$. Moreover, each value t in S is attained exactly $H(t^2 - 256)$ times, where $H(d)$ is the Kronecker class number of d. Hence, we have the following Table 1

By Theorem 15, $T(7) = 3 \cdot 2^{6-4} - 2^{\frac{6}{2}-2} - 1 = 9$, $T(19) = 3 \cdot 2^2 = 12$, $T(11) = 3 \cdot 2^2 + 2^{\frac{6}{2}-2} = 14 = 6 + 8$, and $T(23) = T(19) = 12$. This is in accordance with Table 1 above. The remaining values $T(3)$ and $T(15)$ will be verified in the next subsection.

6.2. *Case $a \neq c^4 + c^3$ for all $c \in \mathbb{F}_q^*$*

Assume $a \neq c^4 + c^3$ for all $c \in \mathbb{F}_q^*$, equivalently $a = b^3$ for some $b \in \mathbb{F}_q$ with $\mathrm{Tr}_2(b) \neq 0$. Let $\epsilon \in \mathbb{F}_2$, let β be an element of $\mathbb{F}_4^*$, and let

$$S_\beta(\epsilon) = \{ b \in \mathbb{F}_q^* \mid \mathrm{Tr}(b^3) = \epsilon,\ \mathrm{Tr}_2(b) = \beta \}.$$

Table 1

t	-13	-9	-5	-1	3	7	11	15
t mod 24	11	15	19	23	3	7	11	15
$H(t^2 - 256)$	6	7	12	12	6	9	8	3

Lemma 17. *The value of $K(b^3)$ modulo 24 corresponding to $\mathrm{Tr}(b^3)=\epsilon$ in Theorem 11 is attained exactly*

$$\frac{1}{3}\sum_{\beta\in\mathbb{F}_4^*}\#S_\beta(\epsilon)$$

times as b varies over $\bigcup_{\beta\in\mathbb{F}_4^*}S_\beta(\epsilon)$.

Proof. Let ζ be a primitive element of $\mathbb{F}_4^*$, and let $\beta\in\mathbb{F}_4^*$. If $b\in S_\beta(\epsilon)$ and $i\in\mathbb{Z}$, then $\mathrm{Tr}((\zeta^i b)^3)=\mathrm{Tr}(b^3)=\epsilon$ and $\mathrm{Tr}_2(\zeta^i b)=\zeta^i\,\mathrm{Tr}_2(b)$, and therefore $\zeta^i b\in S_{\zeta^i\beta}(\epsilon)$. Hence, if $a=b^3$ for some $b\in S_\beta(\epsilon)$, then a has exactly three preimages under the map $x\mapsto x^3$ defined on $\bigcup_{\beta\in\mathbb{F}_4^*}S_\beta(\epsilon)$. This completes the proof. $\square$

Theorem 18. *Let $k\in\{3,15\}$. The number $T(k)$ of elements a in $\mathbb{F}_q^*$ for which $K(a)\equiv k \pmod{24}$ is given by*

m mod 8	$T(3)$	$T(15)$
0	2^{m-3}	2^{m-3}
2, 6	$2^{m-3}-2^{\frac{m}{2}-2}$	$2^{m-3}+2^{\frac{m}{2}-2}$
4	$2^{m-3}+2^{\frac{m}{2}-1}$	$2^{m-3}-2^{\frac{m}{2}-1}$

Proof. Let $\beta\in\mathbb{F}_4^*$, and let ψ and η be the canonical additive characters of $\mathbb{F}_2$ and $\mathbb{F}_4$. The orthogonality of characters implies

$$\begin{aligned}8\cdot\#S_\beta(\epsilon)&=\sum_{x\in\mathbb{F}_q^*}\Bigg(\sum_{u\in\mathbb{F}_2}\psi\big(\big(\mathrm{Tr}\big(x^3\big)+\epsilon\big)u\big)\Bigg)\Bigg(\sum_{v\in\mathbb{F}_4}\eta\big(\big(\mathrm{Tr}_2(x)+\beta\big)v\big)\Bigg)\\&=\sum_{x\in\mathbb{F}_q^*}\big(1+(-1)^\epsilon\chi\big(x^3\big)\big)\sum_{v\in\mathbb{F}_4}\chi(xv)\psi(\beta v).\end{aligned}$$

Now, since $v^3=1$ for $v\in\mathbb{F}_4^*$, we get

$$\begin{aligned}8\sum_{\beta\in\mathbb{F}_4^*}\#S_\beta(\epsilon)&=\sum_{x\in\mathbb{F}_q^*}\big(1+(-1)^\epsilon\chi\big(x^3\big)\big)\sum_{v\in\mathbb{F}_4}\chi(xv)\sum_{\beta\in\mathbb{F}_4^*}\psi(\beta v)\\&=\sum_{x\in\mathbb{F}_q^*}\big(1+(-1)^\epsilon\chi\big(x^3\big)\big)\Bigg(3-\sum_{v\in\mathbb{F}_4^*}\chi(vx)\Bigg)\\&\overset{x\mapsto v^{-1}x}{=}\sum_{x\in\mathbb{F}_q^*}\big(1+(-1)^\epsilon\chi\big(x^3\big)\big)\Bigg(3-\sum_{v\in\mathbb{F}_4^*}\chi(x)\Bigg)\\&=3\sum_{x\in\mathbb{F}_q^*}\big(1+(-1)^\epsilon\chi\big(x^3\big)\big)\big(1-\chi(x)\big).\end{aligned}$$

Since $\sum_{x\in\mathbb{F}_q^*}\chi(x)=-1$, it follows that

$$8\sum_{\beta\in\mathbb{F}_4^*}\#S_\beta(\epsilon)=3\Bigg(q+(-1)^\epsilon\sum_{x\in\mathbb{F}_q^*}\chi\big(x^3\big)-(-1)^\epsilon\sum_{x\in\mathbb{F}_q^*}\chi\big(x^3+x\big)\Bigg).$$

Now, by Lemma 12, we get

$$8\sum_{\beta\in\mathbb{F}_4^*}\#S_\beta(\epsilon)=3\begin{cases} q & \text{if } m\equiv 0 \pmod 8,\\ q+(-1)^\epsilon 2\sqrt{q} & \text{if } m\equiv 2,6 \pmod 8,\\ q-(-1)^\epsilon 4\sqrt{q} & \text{if } m\equiv 4 \pmod 8).\end{cases}$$

Lemma 17 now completes the proof. □

Example 19. Let $m=6$. By Theorem 18, $T(3)=2^{6-3}-2^{\frac{6}{2}-2}=6$ and $T(15)=2^{6-3}+2^{\frac{6}{2}-2}=10=7+3$. This is in accordance with the table in Example 16.

Acknowledgments

The author would like to thank the anonymous referees for their detailed and valuable comments.

References

[1] P. Charpin, T. Helleseth, V. Zinoviev, The divisibility modulo 24 of Kloosterman sums on $GF(2^m)$, m odd, J. Combin. Theory Ser. A 114 (2007) 322–338.
[2] H. Dobbertin, P. Felke, T. Helleseth, P. Rosendahl, Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums, IEEE Trans. Inform. Theory 52 (2006) 613–627.
[3] K. Garaschuk, P. Lisoněk, On binary Kloosterman sums divisible by 3, Des. Codes Cryptogr. 49 (2008) 347–357.
[4] T. Helleseth, V.A. Zinoviev, On $\mathbb{Z}_4$-linear Goethals codes and Kloosterman sums, Des. Codes Cryptogr. 17 (1999) 246–262.
[5] X. Hou, Explicit evaluation of certain exponential sums of binary quadratic functions, Finite Fields Appl. 13 (2007) 843–868.
[6] G. Lachaud, J. Wolfmann, The weights of orthogonals of the extended quadratic binary Goppa codes, IEEE Trans. Inform. Theory 36 (1990) 686–692.
[7] M. Moisio, A note on evaluations of some exponential sums, Acta Arith. 93 (2000) 117–119.
[8] M. Moisio, The moments of a Kloosterman sum and the weight distribution of a Zetterberg type binary cyclic code, IEEE Trans. Inform. Theory 53 (2007) 843–847.
[9] M. Moisio, Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm, Acta Arith. 132 (2008) 329–350.
[10] H. Stichtenoth, Algebraic Function Fields and Codes, Springer, Berlin, 1993.
[11] J. Wolfmann, The number of points on certain algebraic curves, Comm. Algebra 17 (1989) 2055–2060.