Discrete Applied Mathematics 158 (2010) 1064–1072

Contents lists available at ScienceDirect

Discrete Applied Mathematics

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

A transform property of Kloosterman sums

Ian F. Blake [a,*], Theo Garefalakis [b]

[a] Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, BC V6T 1Z4, Canada

[b] Department of Mathematics, University of Crete, 71409 Heraklion, Greece

ARTICLE INFO

Article history:
Received 10 February 2008
Received in revised form 30 December 2009
Accepted 27 February 2010
Available online 1 April 2010

Keywords:
Kloosterman sums
Melas codes
Elliptic curves
Polynomials over finite fields

ABSTRACT

An expression for the number of times a certain trace function associated with a Kloosterman sum on an extension field assumes a given value in the base field is given and its properties explored. The relationship of this result to the enumeration of certain types of irreducible polynomials over fields of characteristic two or three and to the weights in the dual of a Melas code is considered. It is argued that the expressions obtained for the trace functions, while simply related to the Kloosterman sums, can be more directly useful than the exponential sums themselves in certain applications. In addition, they enjoy properties that are of independent interest.

1. Introduction

Let $\mathbb{F}_q$ be the finite field of q elements of characteristic p, and $\mathbb{F}_{q^k}$ its extension of degree k. An additive character χ of $\mathbb{F}_q$ is a complex valued function of unit magnitude with the property that $\chi(\alpha+\beta)=\chi(\alpha)\chi(\beta)$, $\alpha,\beta\in\mathbb{F}_q$. The character [12] is called nontrivial if there exists at least one element of $\mathbb{F}_q$ for which it is not of value 1. Any such character on a field of characteristic p can be realized by the function

$$\chi(\alpha)=\mathrm{e}^{2\pi\mathrm{i}\mathrm{Tr}_{q|p}(a\alpha)/p}$$

for some fixed element $a\in\mathbb{F}_q$ where $\mathrm{Tr}_{q|p}$ is the trace function of $\mathbb{F}_q$ over $\mathbb{F}_p$. Such a character is denoted by $\chi_a(\cdot)$ and the number of distinct characters, including the trivial one, is the order of the finite field. An arbitrary character on $\mathbb{F}_q$ will be denoted simply by $\chi(\cdot)$. An excellent reference for properties of characters and Kloosterman sums as discussed below, is [12], as well as the original work of Carlitz [3] which established many of the properties which are extended here.

Characters satisfy the orthogonality relations:

$$\sum_{c\in F_q}\chi_a(c)\bar{\chi}_b(c)=q\delta_{ab}\quad\text{and}\quad\sum_{b\in F_q}\chi_b(c)\bar{\chi}_b(d)=q\delta_{cd}$$

where δ_{ab} is the Kronecker delta function, equal to one if $a=b$ and 0 otherwise.

A character $\chi(\cdot)$ over $\mathbb{F}_q$ can be 'lifted' to an extension field $\mathbb{F}_{q^k}$ by

$$\chi^{(k)}(\gamma)=\chi(\mathrm{Tr}_{q^k|q}(\gamma))=\exp(2\pi\mathrm{i}\mathrm{Tr}_{q^k|p}(c\gamma)/p),\quad\gamma\in\mathbb{F}_{q^k},\ c\in\mathbb{F}_q.$$

The sums

$$K_1(a,b)=K(a,b)=\sum_{\alpha\in\mathbb{F}_q^*}\chi(a\alpha+b\alpha^{-1})\quad\text{and}\quad K_k(a,b)=\sum_{\gamma\in\mathbb{F}_{q^k}^*}\chi^{(k)}(a\gamma+b\gamma^{-1})$$

* Corresponding address: Department of Electrical and Computer Engineering, University of British Columbia, 2332 Main Mall–Kaiser 4101, Vancouver, BC, V6T 1Z4 Canada. Tel.: +1 604 827 4312; fax: +1 604 822 5949.
E-mail addresses: ifblake@ece.ubc.ca (I.F. Blake), theo@math.uoc.gr (T. Garefalakis).

0166-218X/$ – see front matter
doi:10.1016/j.dam.2010.02.012

for a, b fixed elements of $\mathbb{F}_q$, are referred to as Kloosterman sums [12]. It is noted that some authors allow $a, b \in \mathbb{F}_{q^k}$ in the definition of such sums. This causes no problems but our applications need only the case considered here. In what follows, we assume that $\chi(\cdot)$ is a fixed nontrivial character of $\mathbb{F}_q$ and $ab \neq 0$ since otherwise the sums are trivial. A fundamental result is that

$$K_k(a, b) = -\omega_1^k(a, b) - \omega_2^k(a, b) \tag{1}$$

where $\omega_1(a, b)$, $\omega_2(a, b)$ (or simply ω_1 and ω_2 when the a, b are understood) are complex numbers defined by

$$1 + K(a, b)z + qz^2 = (1 - \omega_1(a, b)z)(1 - \omega_2(a, b)z).$$

It is immediate that

$$K(a, b) = -\omega_1(a, b) - \omega_2(a, b) \quad \text{and} \quad \omega_1(a, b) \cdot \omega_2(a, b) = q.$$

It follows from the Riemann Hypothesis for function fields, that

$$|\omega_1(a, b)| = |\omega_2(a, b)| = \sqrt{q},$$

so that

$$|K(a, b)| \leq 2q^{1/2}.$$

It is interesting to note that $K_k(a, b)$ is entirely determined by the ground field $\mathbb{F}_q$, $K_1(a, b)$ and k.

Furthermore, since

$$\omega_1^k + \omega_2^k = (\omega_1 + \omega_2) \cdot (\omega_1^{k-1} + \omega_2^{k-1}) - q(\omega_1^{k-2} + \omega_2^{k-2}), \quad k \geq 2$$

the following recursion is immediate [3,12]:

$$K_k(a, b) = -K_1(a, b)K_{k-1}(a, b) - qK_{k-2}(a, b) \quad k \geq 2, \qquad K_0(a, b) = -2 \tag{2}$$

which will prove useful in what follows. More generally, by the same argument, we have:

$$K_k(a, b) = -K_s(a, b)K_{k-s}(a, b) - q^s K_{k-2s}(a, b) \quad k \geq 2, \qquad K_0(a, b) = -2, \quad ab \neq 0, \ 1 \leq s \leq \lfloor k/2 \rfloor. \tag{3}$$

For $k = 2\ell$ the last equation gives

$$K_{2\ell}(a, b) = -K_\ell^2(a, b) + 2q^\ell.$$

We adopt the convention that $K_k(a, a) = K_k(a)$. The ground field will be assumed $\mathbb{F}_q$ and note that $K_k(0, 0) = K_k(0) = q^k - 1$.

A further identity, which shows explicitly the dependence of $K_k(a, b)$ only on $\mathbb{F}_q$ and $K_1(a, b)$ (again, assuming a fixed nontrivial character $\chi(\cdot)$) is [3,12]

$$K_k(a, b) = \sum_{j=0}^{\lceil k/2 \rceil} (-1)^{k-j-1} \frac{k}{k-j} \binom{k-j}{j} q^j K_1^{k-2j}(a, b), \quad ab \neq 0. \tag{4}$$

Such Kloosterman sums have been widely investigated for a variety of applications in coding, sequence design, equations over finite fields and many others (see e.g. [6,11,19]). In the next section we derive a formula that gives the number of times each element of $\mathbb{F}_q$ is assumed as a value of a term in a Kloosterman sum evaluated over $\mathbb{F}_{q^k}$. This adds, for example, to the work of Katz and Livné [9], which gives results for the case $q = 2$ and 3 in terms of orders in certain algebraic number fields. The approach here seems more direct than that work. Such numbers will be shown to have properties similar to those of the Kloosterman sums themselves and are of independent interest in applications.

Sections 3 and 4 consider the application of this result to two problems; (i) enumerating irreducible polynomials with a certain type of restriction on their coefficients (ii) the possible weights in the duals of Melas codes over $\mathbb{F}_q$. The work is an extension of work initiated in [1] where the interest was in determining the order of the additive group of elliptic curves over finite fields of characteristic two. The relationship of that work to that of Section 4 is touched on there.

2. A result on the values of Kloosterman sums

Consider first, for fixed $a, b \in \mathbb{F}_q$, the set of elements γ in $\mathbb{F}_{q^k}$ such that

$$S_k(\beta, a, b) = \{\gamma \in \mathbb{F}_{q^k} | \mathrm{Tr}_{q^k|q}(a\gamma + b\gamma^{-1}) = \beta\}, \quad a, b, \beta \in \mathbb{F}_q$$

and let $n_k(\beta, a, b) = |S_k(\beta, a, b)|$ where $\mathrm{Tr}_{q^k|q}(\cdot)$ is the trace function of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$. In what follows, we will often take $n_k(\beta, 1, 1) \triangleq n_k(\beta)$. A few easy observations are recorded below.

Proposition 1. *Let $\mathbb{F}_q$ be a finite field of characteristic p, $a, b, c, \beta \in \mathbb{F}_q$. Then*

(1) $\gamma \in S_k(\beta, a, b) \Longrightarrow \gamma^q \in S_k(\beta, a, b)$.
(2) $n_k(\beta, a, b) = n_k(-\beta, a, b)$.

(3) *If* $a \neq 0$ *then* $n_k(\beta, a, a) = n_k(\beta a^{-1}, 1, 1)$.
(4) *If* $c \neq 0$ *then* $n_k(\beta, ca, cb) = n_k(\beta c^{-1}, a, b)$.
(5) $n_k(\beta^p, a^p, b^p) = n_k(\beta, a, b)$.

Our main interest will later be in the quantities $K_k(1, 1)$, although the proofs will be given for the general case. The following theorem establishes the basic transform relationship between the Kloosterman sums and the quantities $n_k(\beta, a, b)$.

Theorem 1. *Let* $a, b, c \in \mathbb{F}_q^*$, *and* $K_k(a, b)$ *the Kloosterman sum associated to a nontrivial additive character* χ *of* $\mathbb{F}_q$. *Then*

$$K_k(ca, cb) = \sum_{\eta \in \mathbb{F}_q} n_k(\eta, a, b)\chi(c\eta) \tag{5}$$

and

$$n_k(\beta, a, b) = \frac{1}{q} \sum_{c \in \mathbb{F}_q} \bar{\chi}(c\beta) K_k(ca, cb). \tag{6}$$

Proof. For the first part of the theorem, for $c = 1$, we see that

$$K_k(a, b) = \sum_{\gamma \in \mathbb{F}_{q^k}^*} \chi(\mathrm{Tr}_{q^k|q}(a\gamma + b\gamma^{-1})) = \sum_{\beta \in \mathbb{F}_q} n_k(\beta, a, b)\chi(\beta).$$

More generally,

$$\begin{aligned} K_k(ca, cb) &= \sum_{\beta \in \mathbb{F}_q} n_k(\beta, ca, cb)\chi(\beta) \\ &= \sum_{\beta \in \mathbb{F}_q} n_k(\beta c^{-1}, a, b)\chi(\beta) \\ &= \sum_{\eta \in \mathbb{F}_q} n_k(\eta, a, b)\chi(c\eta), \end{aligned}$$

where we used Proposition 1 in the second equality.

For the second part of the theorem, to determine the quantities $n_k(\beta, a, b)$ let $\chi(\cdot)$ denote the a nontrivial character of $\mathbb{F}_q$ and consider the sum

$$\sum_{\gamma \in \mathbb{F}_{q^k}^*} \left\{ \sum_{c \in \mathbb{F}_q} \chi(c(\mathrm{Tr}_{q^k|q}(a\gamma + b\gamma^{-1}) - \beta)) \right\}. \tag{7}$$

If γ is such that $\mathrm{Tr}_{q^k|q}(a\gamma + b\gamma^{-1}) = \beta$ then the inner sum is q and otherwise 0. Thus the expression of Eq. (7) is $qn_k(\beta, a, b)$ and so

$$\begin{aligned} n_k(\beta, a, b) &= \frac{1}{q} \sum_{\gamma \in \mathbb{F}_{q^k}^*} \left\{ \sum_{c \in \mathbb{F}_q} \chi(c(\mathrm{Tr}_{q^k|q}(a\gamma + b\gamma^{-1}) - \beta)) \right\} \\ &= \frac{1}{q} \sum_{\gamma \in \mathbb{F}_{q^k}^*} \sum_{c \in \mathbb{F}_q} \chi(c\mathrm{Tr}_{q^k|q}(a\gamma + b\gamma^{-1})\bar{\chi}(c\beta)) \qquad (8) \\ &= \frac{1}{q} \sum_{c \in \mathbb{F}_q} \bar{\chi}(c\beta) \sum_{\gamma \in \mathbb{F}_{q^k}^*} \chi(c\mathrm{Tr}_{q^k|q}(a\gamma + b\gamma^{-1})) \\ &= \frac{1}{q} \sum_{c \in \mathbb{F}_q} \bar{\chi}(c\beta) \sum_{\gamma \in \mathbb{F}_{q^k}^*} \chi^{(k)}(c(a\gamma + b\gamma^{-1})) \\ &= \frac{1}{q} \sum_{c \in \mathbb{F}_q} \bar{\chi}(c\beta) K_k(ca, cb). \quad \square \qquad (9) \end{aligned}$$

From the theorem it is emphasized that the quantities $n_k(\beta, a, b)$ can be obtained using only knowledge of $K_1(a, b)$ over $\mathbb{F}_q$ and k. Furthermore the sets of quantities $\{n_k(\beta, a, b), \beta \in \mathbb{F}_q\}$ and $\{K_k(ca, \eta b), c \in \mathbb{F}_q\}$ are a type of transform of each other via Eqs. (5) and (6). As such they enjoy many transform-like properties, some of which will be explored below. The quantities and their properties are of independent interest and useful in many applications.

The following corollaries emphasize this point of view by emulating multiplication and convolution in the two domains.

Corollary 1. *Let $a, b \in \mathbb{F}_q^*$ and $c, \beta \in \mathbb{F}_q$. Then*

$$\frac{1}{q}\sum_{c\in\mathbb{F}_q} \bar{\chi}(c\beta)K_k^2(ca, cb) = \sum_{\eta\in\mathbb{F}_q} n_k(\eta, a, b)n_k(\beta-\eta, a, b), \tag{10}$$

$$\sum_{\beta\in\mathbb{F}_q} \chi(c\beta)n_k^2(\beta, a, b) = \frac{1}{q}\sum_{d\in\mathbb{F}_q} K_k(da, db)K_k((c-d)a, (c-d)b). \tag{11}$$

Proof. To prove Eq. (10), we compute

$$\begin{aligned} q\sum_{\eta\in\mathbb{F}_q} n_k(\eta, a, b)n_k(\beta-\eta, a, b) &= q\sum_{\eta\in\mathbb{F}_q}\frac{1}{q}\sum_{c\in\mathbb{F}_q}\bar{\chi}(c\eta)K_k(ca, cb)\frac{1}{q}\sum_{d\in\mathbb{F}_q}\bar{\chi}(d(\beta-\eta))K_k(da, db)\\ &= \frac{1}{q}\sum_{c\in\mathbb{F}_q}\sum_{d\in\mathbb{F}_q}\bar{\chi}(d\beta)K_k(ca, cb)K_k(da, db)\sum_{\eta\in\mathbb{F}_q}\bar{\chi}((c-d)\eta). \end{aligned}$$

The sum over η equals q when $c = d$ and zero otherwise and the statement follows. The proof of Eq. (11) is completely analogous. □

The following corollary tries to emulate the recursion relations for the $K_k(a, b)$ of Eq. (3) in the transform domain.

Corollary 2. *Let $a, b \in \mathbb{F}_q^*$ and $\beta \in \mathbb{F}_q$. Then for $1 \le s \le \lfloor k/2 \rfloor$*

$$\begin{aligned} n_k(\beta, a, b) &= -\sum_{\eta\in\mathbb{F}_q} n_{k-s}(\eta, a, b)n_s(\beta-\eta, a, b) + q^s n_{k-2s}(\beta, a, b)\\ &\quad + 2q^{s-1}(q^{k-s}-1), \quad k \ge 2, \qquad qn_0(\beta, a, b) = -2, \quad ab \ne 0. \end{aligned}$$

Proof. Although the proof is elementary, using standard transform techniques, we give an outline of it, recalling that to use Eq. (3) we require $ab \ne 0$:

$$\begin{aligned} n_k(\beta, a, b) &= \frac{1}{q}\sum_{c\in\mathbb{F}_q}\bar{\chi}(c\beta)K_k(ca, cb)\\ &= \frac{1}{q}\sum_{c\in\mathbb{F}_q^*}\bar{\chi}(c\beta)K_k(ca, cb) + \frac{1}{q}(q^k-1)\\ &= \frac{1}{q}\sum_{c\in\mathbb{F}_q^*}\bar{\chi}(c\beta)\left\{-K_s(ca, cb)K_{k-s}(ca, cb) - q^s K_{k-2s}(ca, cb)\right\} + \frac{1}{q}(q^k-1) \end{aligned}$$

and

$$n_k(\beta, a, b) = -\frac{1}{q}\sum_{c\in\mathbb{F}_q^*}\bar{\chi}(c\beta)K_s(ca, cb)K_{k-s}(ca, cb) - q^{s-1}\sum_{c\in\mathbb{F}_q^*}\bar{\chi}(c\beta)K_{k-2s}(ca, cb) + \frac{1}{q}(q^k-1). \tag{12}$$

The rest of the proof is repeated use of the first part of Theorem 1 and the fact that $K_k(0, 0) = q^k - 1$. The second sum in Eq. (12) is then:

$$-q^{s-1}\left\{\sum_{c\in\mathbb{F}_q}\bar{\chi}(c\beta)K_{k-2s}(ca, cb) - \bar{\chi}(0)K_{k-2s}(0, 0)\right\} = -q^s n_{k-2s}(\beta, a, b) + q^{s-1}(q^{k-2s}-1).$$

The first sum in Eq. (12) is:

$$
\begin{aligned}
-\frac{1}{q}\sum_{c\in\mathbb{F}_q^*}\bar{\chi}(c\beta)K_s(ca,cb)K_{k-s}(ca,cb) &= -\frac{1}{q}\sum_{c\in\mathbb{F}_q^*}\bar{\chi}(c\beta)K_s(ca,cb)\left\{\sum_{\eta\in\mathbb{F}_q} n_{k-s}(\eta,a,b)\chi(c\eta)\right\}\\
&= -\frac{1}{q}\sum_{\eta\in\mathbb{F}_q} n_{k-s}(\eta,a,b)\left\{\sum_{c\in\mathbb{F}_q}\chi(c(\eta-\beta))K_s(ca,cb)-\chi(0)K_s(0,0)\right\}\\
&= \sum_{\eta\in\mathbb{F}_q} n_{k-s}(\eta,a,b)\left\{-\frac{1}{q}\sum_{c\in\mathbb{F}_q}\bar{\chi}(c(\beta-\eta))K_s(ca,cb)\right\}+\frac{1}{q}(q^s-1)\sum_{\eta\in\mathbb{F}_q} n_{k-s}(\eta,a,b)\\
&= -\sum_{\eta\in\mathbb{F}_q} n_{k-s}(\eta,a,b)n_s(\beta-\eta,a,b)+\frac{1}{q}(q^s-1)(q^{k-s}-1).
\end{aligned}
$$

The sum of all three terms in the original equation gives the result of the corollary. □

The only other result of a similar nature known to the authors is that in [9] which relates $n_k(\beta)=n_k(\beta,1,1)$ to a summation of a certain function over orders in an algebraic number field containing the ring of its integers for the cases of $q=2$ or 3. The generality and simplicity of the above corollaries is appealing.

Theorem 1 allows for good estimates for the values $n_k(\beta,a,b)$, which we state as a corollary, a kind of equidistribution property.

Corollary 3. *Let, $a,b,\beta\in\mathbb{F}_q$. Then*

$$
\begin{aligned}
n_k(\beta,0,0) &= \begin{cases} q^k-1, & \text{if } \beta=0\\ 0, & \text{if } \beta\neq 0\end{cases}\\
|n_k(\beta,a,b)-q^{k-1}| &\le 2q^{\frac{k}{2}}, \quad \text{if } ab\neq 0.
\end{aligned}
$$

Proof. The first statement follows immediately from the definition of Kloosterman sums. For the estimate in the case $ab\neq 0$, we use Theorem 1. The main contribution comes from the term corresponding to $c=0$ and the remaining terms are bounded by $2q^{\frac{k}{2}}$. □

3. Application to the enumeration of certain polynomials

The enumeration of certain irreducible polynomials over $\mathbb{F}_q$ is considered. The enumeration of irreducible polynomials such that certain coefficients are chosen independently has been of great interest in recent literature (see [5,21] for recent work on such results). Our purpose here is to observe that the results of the previous section have an application here, although the condition of interest is somewhat artificial. Suppose that

$$X^k+c_1X^{k-1}+\cdots+c_{k-1}X+c_k\in\mathbb{F}_q[X]$$

is irreducible over $\mathbb{F}_q$ and let γ be a root of the polynomial in $\mathbb{F}_{q^k}$. Note that $c_1+c_{k-1}/c_k=-\mathrm{Tr}_{q^k|q}(\gamma+\gamma^{-1})$. The set $S_k(\beta)$ defined earlier is then the set of roots of all monic irreducible polynomials over $\mathbb{F}_q$ whose degrees divide k with the property that the second coefficient plus the ratio of the last two coefficients is β. While this condition is somewhat artificial in comparison to setting the coefficients arbitrarily in $\mathbb{F}_q$, it nonetheless seems of interest that the enumeration of such polynomials follows directly from the previous results.

If $\gamma\in S_k(\beta)$ is a root of a monic irreducible polynomial over $\mathbb{F}_q$ of degree $d|k$ then

$$\mathrm{Tr}_{q^k|q}(\gamma+\gamma^{-1})=\frac{k}{d}\mathrm{Tr}_{q^d|q}(\gamma+\gamma^{-1}).$$

Let $R_k(\beta)=\{\gamma\in S_k(\beta):\deg(\gamma)=k\}$ be the subset of $S_k(\beta)$ of elements of degree k. Then it is not hard to see that

$$
\begin{aligned}
S_k(\beta) &= \bigcup_{d|k} R_d\left(\frac{d}{k}\beta\right), \quad \text{if } (k,q)=1\\
S_k(\beta) &= \bigcup_{\substack{d|k\\ \left(\frac{k}{d},q\right)=1}} R_d\left(\frac{d}{k}\beta\right), \quad \text{if } \left(\frac{k}{d},q\right)>1 \text{ and } \beta\neq 0\\
S_k(0) &= \bigcup_{\substack{d|k\\ \left(\frac{k}{d},q\right)=1}} R_d(0)\bigcup_{c\in\mathbb{F}_q}\bigcup_{\substack{d|k\\ \left(\frac{k}{d},q\right)>1}} R_d(c) \quad \text{if } (k,q)>1.
\end{aligned}
$$

Denoting $r_d(\beta) = |R_d(\beta)|$, we have

$$n_k(\beta) = \begin{cases} \displaystyle\sum_{d|k} r_d\left(\frac{d}{k}\beta\right), & \text{if } (k,q)=1, \\ \displaystyle\sum_{\substack{d|k \\ \left(\frac{k}{d},q\right)=1}} r_d\left(\frac{d}{k}\beta\right), & \text{if } (k,q)>1 \text{ and } \beta\neq 0 \\ \displaystyle\sum_{\substack{d|k \\ \left(\frac{k}{d},q\right)=1}} r_d(0) + \sum_{c\in\mathbb{F}_q} \sum_{\substack{d|k \\ \left(\frac{k}{d},q\right)>1}} r_d(c), & \text{if } (k,q)>1 \text{ and } \beta=0 \end{cases}$$

which is equivalent to

$$n_k(\beta) = \begin{cases} \displaystyle\sum_{\substack{d|k \\ \left(\frac{k}{d},q\right)=1}} r_d\left(\frac{d}{k}\beta\right), & \text{if } \beta\neq 0 \\ \displaystyle\sum_{\substack{d|k \\ \left(\frac{k}{d},q\right)=1}} r_d(0) + \sum_{c\in\mathbb{F}_q} \sum_{\substack{d|k \\ \left(\frac{k}{d},q\right)>1}} r_d(c), & \text{if } \beta=0. \end{cases}$$

Suppose now that $(k,q)=1$ and $\beta=0$. Then

$$n_k(0) = \sum_{d|k} r_d(0),$$

and the Möbius inversion formula gives

$$r_k(0) = \sum_{d|k} \mu\left(\frac{k}{d}\right) n_d(0).$$

Proposition 2. *Let q be a prime power and $k\in\mathbb{N}$ with $(k,q)=1$. The number, $I_{q,k}(0)$, of irreducible polynomials of degree k of the form $f = X^k + c_1X^{k-1} + \cdots + c_{k-1}X + c_k \in \mathbb{F}_q[X]$ with $c_1 + c_{k-1}/c_k = 0$ is given by*

$$I_{q,k}(0) = \frac{1}{k}\sum_{d|k} \mu\left(\frac{k}{d}\right) n_d(0) = \frac{1}{kq}\sum_{c\in\mathbb{F}_q}\sum_{d|k} \mu\left(\frac{k}{d}\right) K_d(c,c).$$

In particular,

$$\left| I_{q,k}(0) - \frac{q^{k-1}}{k} \right| \leq \frac{3q^{\frac{k}{2}}}{k}.$$

Proof. It suffices to observe that $I_{q,k}(0) = \frac{1}{k}r_k(0)$, and make use of Theorem 1. For the stated bound, we compute

$$\begin{aligned} I_{q,k}(0) &= \frac{1}{kq}\sum_{c\in\mathbb{F}_q}\sum_{d|k} \mu\left(\frac{k}{d}\right) K_d(c,c) \\ &= \frac{1}{kq}\left(\sum_{d|k} \mu\left(\frac{k}{d}\right) K_d(0,0) + \sum_{c\in\mathbb{F}_q^*}\sum_{d|k} \mu\left(\frac{k}{d}\right) K_d(c,c)\right) \\ &= \frac{1}{kq}\left(q^k - 1 + \sum_{\substack{d|k \\ d<k}} \mu\left(\frac{k}{d}\right) K_k(0,0) + \sum_{c\in\mathbb{F}_q^*}\sum_{d|k} \mu\left(\frac{k}{d}\right) K_d(c,c)\right). \end{aligned}$$

Therefore,

$$\begin{aligned} \left| I_{q,k}(0) - \frac{q^{k-1}}{k} \right| &\leq \frac{1}{kq}\left(1 + \sum_{\substack{d|k \\ d<k}} (q^d - 1) + (q-1)\sum_{d|k} 2q^{\frac{d}{2}}\right) \\ &\leq \frac{1}{kq}\left(q\frac{q^{\frac{k}{2}} - 1}{q-1} + 2(q-1)\frac{q^{\frac{k}{2}+1} - q^{\frac{1}{2}}}{q-1}\right) \end{aligned}$$

$$\leq \frac{q^{\frac{k}{2}}}{kq}\frac{2q^2-q}{q-1}$$
$$\leq \frac{3q^{\frac{k}{2}}}{k}.$$

We note that the coefficient 3 is an upper bound for $(2q-1)/(q-1)$. For $q>2$ it can be substituted by $5/2$. □

Proposition 3. *Let q be a power of $p \in \{2,3\}$, $k \in \mathbb{N}$, and $\beta \in \mathbb{F}_q^*$. Write $k = p^e m$, $(m,p)=1$. Then the number of irreducible polynomials of degree k of the form $f = X^k + c_1X^{k-1} + \cdots + c_{k-1}X + c_k \in \mathbb{F}_q[X]$, with $c_1 + c_{k-1}/c_k = \beta$ is given by*

$$I_{q,k}(\beta) = \frac{1}{k}\sum_{d|m}\mu\left(\frac{m}{d}\right)n_{p^e d}(\beta).$$

In particular,

$$\left|I_{q,k}(\beta) - \frac{q^{k-1}}{k}\right| \leq \frac{3q^{\frac{k}{2}}}{k}.$$

Proof. We start from

$$n_k(\beta) = \sum_{\substack{d|k \\ \left(\frac{k}{d},q\right)=1}} r_d\left(\frac{k}{d}\beta\right).$$

Since we are in a field of characteristic 2 or 3, and $\left(\frac{k}{d},q\right)=1$, we have $\frac{k}{d}\beta = \pm\beta$. It is not hard to see that $r_{p^e d}(-\beta) = r_{p^e d}(\beta)$. So the equation becomes

$$n_{p^e m}(\beta) = \sum_{\substack{d|k \\ \left(\frac{k}{d},q\right)=1}} r_d(\beta) = \sum_{d|m} r_{p^e d}(\beta)$$

and by Möbius inversion we get

$$r_{p^e m}(\beta) = \sum_{d|m}\mu\left(\frac{m}{d}\right)n_{p^e d}(\beta),$$

which proves the first statement. For the second estimate, we compute

$$I_k(\beta) = \frac{1}{k}n_k(\beta) + \frac{1}{k}\sum_{\substack{d|m \\ d<m}}\mu\left(\frac{m}{d}\right)n_{p^e d}(\beta).$$

The main contribution comes from $\frac{1}{k}n_k(\beta)$. Using the estimate of Corollary 3, we get the stated bound. □

Note there are many works which enumerate or bound the number of irreducible polynomials of given degree with certain fixed coefficients. For example, the number of irreducible polynomials of degree k of the form $f(x) = x^k - ax^{k-1} + \cdots + (-1)^k b$ over $\mathbb{F}_q$, $b \neq 0$, $P_k(a,b)$ is bounded by

$$\left|P_k(a,b) - \frac{q^{k-1}}{k(q-1)}\right| \leq \frac{3}{k}q^{k/2}.$$

In this bound, two coefficients are fixed, a and b. The bounds of the previous two propositions however, although involving three coefficients, c_1, c_{k-1} and c_k, are actually fixing the equivalent of a single coefficient. To justify this, consider the set of all irreducible polynomials over $\mathbb{F}_q$, approximately q^k/k of them. Under a random hypothesis on the behavior of the quantities $c_1 + c_{k-1}/c_k$, computed for each such polynomial, one might reasonably assume an approximate equidistribution of such quantities. Consequently, under such an assumption, each value of $\mathbb{F}_q$ would appear approximately $q^k/qk = q^{k-1}/k$ times, as the propositions imply.

4. Application to the weights of the dual of a Melas code

Let α be a primitive element of $\mathbb{F}_{q^m}^*$ and define the code $C(q^m)$ over $\mathbb{F}_{q^m}$ to have the parity check matrix

$$H(q^m) = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{q^m-2} \\ 1 & \alpha^{-1} & \alpha^{-2} & \cdots & \alpha^{-(q^m-2)} \end{bmatrix}$$

i.e. $C(q^m)$ is the cyclic code over $\mathbb{F}_q$ with generator polynomial $m_\alpha(x)m_{\alpha_{-1}}(x)$, the product of the minimal polynomials of α and α^{-1} over $\mathbb{F}_q$, respectively.

Define the dual of the Melas code over $\mathbb{F}_q$ as $M(q)$ where

$$M(q) = (C(q^m)|_{\mathbb{F}_q})^\perp = \mathrm{Tr}_{\mathbb{F}_{q^m}|\mathbb{F}_q}(C(q^m)^\perp)$$

where the right-hand equality follows from Delsarte's Theorem. Thus for $a, b \in \mathbb{F}_q$ the codeword $c(a, b) \in M(q)$ can be expressed as

$$c(a, b) = (c_0, c_1, \ldots, c_{q^m-2}), \qquad c_j = \mathrm{Tr}_{\mathbb{F}_{q^m}|\mathbb{F}_q}(a\alpha^j + b\alpha^{-j}), \quad j = 0, 1, \ldots, q^m - 2.$$

Thus the codes are of length $(q^m - 1)$ and dimension $2m$ over $\mathbb{F}_q$.

These codes have received considerable attention in the literature, especially for the case of $q = 2$ and $q = 3$ [10,11, 16,18,17]. Excellent general references are [7,8]. The relationship of the weight enumerator problem for these codes in the case of characteristic two and elliptic curves is examined in several works, including [11,18,17], which contain many deep, elegant and interesting results using this approach. A brief comment on this is given below. In particular the work of [18] is able to determine the weight enumerator of the binary Melas code of length $2^m - 1$, in terms of the traces of certain Hecke operators acting on spaces of cusp forms for the congruence subgroup $\Gamma_1(4) \in SL_2(\mathbb{Z})$.

While most of these works consider the codes over the characteristic subfield, either $\mathbb{F}_2$ [8,11], $\mathbb{F}_3$ [20] or $\mathbb{F}_p$ [7], our interest is the case of arbitrary field $\mathbb{F}_q$ as in [16]. It can be shown the code C_2 in [16] is our code $M(q)$ for arbitrary q. That paper also considers a closely related $(q^m + 1, 2m)$ code over $\mathbb{F}_q$ which could also be considered with the techniques used here. For reasons of space we do not. Both of these codes are easily shown to be unions of simplex-type codes.

Our goal in this section is make the observation that Theorem 2 in [16], follows in a very direct manner from the results of this work. Namely it is immediate that the Hamming weight $w(c(a, b))$ of a codeword $c(a, b) \in M(q)$ is just the codeword length less the number of zero elements for a given $a,\ b$ i.e. $n_k(0, a, b)$, as given in the second part of the theorem:

$$\begin{aligned} w(c(a, b)) &= q^m - 1 - n_m(0, a, b) \\ &= q^m - 1 - \frac{1}{q}\sum_{c\in\mathbb{F}_q} K_m(ca, cb) \\ &= \frac{q-1}{q}(q^m - 1) - \frac{1}{q}\sum_{c\in\mathbb{F}_q^*} K_m(ca, cb) \end{aligned}$$

where the last equation follows from observing that the $c = 0$ term in the summation is

$$\frac{1}{q}(q^m - 1)$$

which gives the result is Theorem 2 in [16]. Theorem 1 in that work follows in a similar manner. The simple and direct manner of this proof, using the quantities $n_k(\beta, a, b)$ and their properties, compared to the original in [16], is appealing. It is noted that the weight distribution results of Corollary 3 give the range of allowable weights for $M(q)$ as in Theorem 3 of [16].

In addition, many results are known concerning the values of Kloosterman sums. In the characteristic 2 case for example, it is known that

$$K_k(a, b) \equiv 3 (\mathrm{mod}\ 4)$$

which gives further information on possible weights in the code. Further such relationship are explored in [4,14], among many other such works.

Notice that although knowledge of the quantities will give the weight enumerator (even the complete weight enumerator [13]) of the code, over any extension field, [18] was able to give an explicit weight enumerator for the case $q = 2$.

While it is clear that any computation with the quantities $n_k(\beta, a, b)$ will in some sense be equivalent to a derivation involving the Kloosterman sums, it seems useful in many situations to use the quantities n_k directly.

Mention has been made on the relationship between Kloosterman sums and the orders of elliptic curves over fields of characteristic two. Indeed this was the original motivation for considering this problem [1]. As many authors have made use of this relationship (e.g. [1,4,6,9,11,10,15,18,17,20]) a brief indication of the relationship is given here.

There are $2(q - 1)$ non-isomorphic classes of elliptic curves over fields of characteristic two [2] and representatives of these classes may be taken as the equations:

$$y^2 + xy = x^3 + a_2x^2 + a_6, \quad a_2,\ a_6 \in \mathbb{F}_q,\ q = 2^m$$

where $a_2 \in \{0, \gamma\}$ and γ an element of trace 1 (of $\mathbb{F}_q$ over $\mathbb{F}_2$). Considering only the case of $a_2 = 0$ (the other case is as easily handled), the resulting equation is transformed to

$$z^2 + z = \sqrt[4]{a_6}u + \frac{\sqrt{a_6}}{u^2}$$

where $y = xz$, $x \neq 0$ and set $x = \sqrt[4]{a_6}u$ (squaring in a field of characteristic 2 is an isomorphism). The equation will have two distinct solutions iff

$$Tr_{q^k|2}\left(\sqrt[4]{a_6}(u + u^{-1})\right) = 0, \tag{13}$$

which relates the order of the additive group of the elliptic curve to Kloosterman sums. Such a relationship was used to advantage (in for example [17] and others), using further properties of elliptic curves, to determine the weight enumerator and other properties of the Melas code described above.

5. Comments

The number of times a certain trace function over $\mathbb{F}_{q^k}$ takes on a given value in $\mathbb{F}_q$ has been investigated and shown to have interesting transform-like properties. As examples of the use of such quantities they were used to determine the number of irreducible polynomials over $\mathbb{F}_q$ that satisfy a certain condition on its coefficients. Additionally they provided a direct and simple proof of previously known results on the weights of the duals of q-ary Melas codes.

The applications support the view that the quantities investigated in the work, $n_k(\beta, a, b)$, can be of more direct usefulness in many problems than the exponential sums themselves. In addition, these quantities themselves have interesting properties, of independent interest, some of which have been considered in this work.

Acknowledgement

The authors would like to thank the anonymous reviewer for providing very useful comments on the original version of the paper.

References

[1] I.F. Blake, G. Seroussi, Ron Roth, On the solutions of an elliptic curve over a field of characteristic two, in: Proceedings Int'l. Symp. Information Theory, Cambridge, MA, 1998.
[2] I.F. Blake, G. Seroussi, N. Smart, Elliptic Curves in Cryptography, in: Lecture Note Series, vol. 265, Cambridge University Press, 1999.
[3] L. Carlitz, Kloosterman sums and finite field extensions, Acta Arithmetica XVI (1969) 179–193.
[4] P. Charpin, T. Helleseth, V. Zinoviev, The divisibility modulo 24 of Kloosterman sums on $GF(2^m)$, m odd, Journal of Combinatorial Theory, Series A 114 (2007) 322–338.
[5] Stephen D. Cohen, Explicit theorems on generator polynomials, Finite Fields and their Applications 11 (2005) 337–357.
[6] Tor Helleseth, Victor Zinoviev, On a new identity for Kloosterman sums and nonlinear system of equations over finite fields of characteristic 2, Discrete Mathematics 274 (2004) 109–124.
[7] T. Hiramatsu, G. Köhler, Coding Theory and Number Theory, Kluwer Academic Publishers, 2003.
[8] Norman E. Hurt, Exponential sums and coding theory: a review, Acta Applicandae Mathematicae 46 (1997) 49–91.
[9] Nicholas Katz, Ron Livné, Sommes Kloosterman et courbes elliptiques universelles en caractéristiques 2 et 3, Comptes Rendus de l'Academie des Sciences, Série I 309 (1989) 723–726.
[10] Gilles Lachaud, Distribution of the weights of the dual of the Melas code, Discrete Mathematics 79 (1989) 103–108.
[11] Gilles Lachaud, Jacques Wolfmann, Sommes de Kloosterman, courbes elliptiques et codes cycliques en caractéristique 2, Comptes Rendus de l'Academie des Sciences, Série I 305 (1987) 881–883.
[12] R. Lidl, H. Niederreiter, Finite Fields, 2nd ed., Cambridge University Press, Cambridge, UK, 1997.
[13] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error Correcting Codes, North Holland, 1977.
[14] Marko Moisio, The divisibility modulo 24 of Kloosterman sums on $GF(2^m)$, m even, Finite Fields and their Applications 15 (2009) 174–184.
[15] Marko Moisio, Kloosterman sums, elliptic curves and irreducible polynomials with prescribed trace and norm, Acta Arithmetica 132 (2008) 329–350.
[16] J.C.C.M. Remin, H.J. Tiersma, A duality theorem for the weight distribution of some cyclic codes, IEEE Transactions on Information Theory 14 (1988) 1348–1352.
[17] René Schoof, Families of codes and weight distributions of codes, Bulletin of the American Mathematical Society 32 (1995) 171–183.
[18] René Schoof, Marcel van der Vlugt, Hecke operators and the weight distributions of certain codes, Journal of Combinatorial Theory, Series A 57 (1991) 163–186.
[19] Dong-Joon Shin, Wonjin Sung, A new Kloosterman sum identity over $\mathbb{F}_{2^m}$ for odd m, Discrete Mathematics 268 (2003) 337–341.
[20] J. Wolfmann, The weights of the dual code of the Melas code over GF(3), Discrete Mathematics 74 (2003) 327–329.
[21] Joseph L. Yucas, Gary L. Mullen, Irreducible polynomials over GF(2) with prescribed coefficients, Discrete Mathematics 274 (2004) 265–279.