A note on Kloosterman sums

Ian F. Blake

Department of Electrical and Computer Engineering University of Toronto, Toronto, ON M5S 3G4, Canada

Theo Garefalakis

Department of Mathematics, University of Crete, 71409 Heraklion, Greece

Abstract

An expression for the number of times a certan 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 number of points on certain elliptic curves and to the enumeration of certain types of irreducible polynomials is considered.

Key words: Kloosterman sums, elliptic curves, polynomials over finite fields

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 [9] 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

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

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

Email addresses: ifblake@comm.toronto.edu (Ian F. Blake), theo@math.uoc.gr (Theo Garefalakis).

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 [9], 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

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

The sums

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

for a, b fixed elements of $\mathbb{F}_q$, are referred to as Kloosterman sums [9]. In the sequel 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

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

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 [3,9]:

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

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

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

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 [3,9]

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

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 [5,**?**,**?**]). 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 Kloosterman sum evaluated over $\mathbb{F}_{q^k}$. This adds, for example, to the work of Katz and Livné [6], which gives results for the case $q = 2$ and 3. Such numbers will be shown to have properties similar to those of the Kloosterman sums themselves.

Section 3 considers the interpretation of this result to two problems; (i) interpreting the result in terms of point counting on elliptic curves. (ii) enumerating irreducible polynomials with a certain type of restriction on their coefficients. The work is an extension of work initiated in [2].

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 $\mathbb{F}_q$. 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) $n_k(\beta^p,a^p,b^p)=n_k(\beta,a,b)$.

While our main interest will later be in the quantities $K_k(1,1)$, proofs will be given for the general case.

Theorem 1 *Let $a,b,c\in\mathbb{F}_q$, $c\neq 0$ and $K_k(a,b)$ the Kloosterman sum associated to a non-trivial additive character χ of $\mathbb{F}_q$. Then*

$$1.\quad K_k(ca,cb)=\sum_{\eta\in\mathbb{F}_q}n_k(\eta,a,b)\chi(c\eta). \tag{5}$$

and

$$2.\quad n_k(\beta,a,b)=\frac{1}{q}\sum_{c\in\mathbb{F}_q}\bar{\chi}(c\beta)K_k(ca,cb) \tag{6}$$

$$=-\frac{1}{q}\sum_{c\in\mathbb{F}_q}\bar{\chi}(c\beta)(\omega_1(ca,cb)^k+\omega_2(ca,cb)^k) \tag{7}$$

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

$$\sum_{\gamma \in \mathbb{F}^*_{q^k}} \{ \sum_{c \in \mathbb{F}_q} \chi(c(\mathrm{Tr}_{q^k|q}(a\gamma + b\gamma^{-1}) - \beta))\} \ . \tag{8}$$

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 Equation (8) is $qn_k(\beta, a, b)$ and so

$$\begin{aligned}
n_k(\beta, a, b) &= \frac{1}{q} \sum_{\gamma \in \mathbb{F}^*_{q^k}} \{ \sum_{c \in \mathbb{F}_q} \chi(c(\mathrm{Tr}_{q^k|q}(a\gamma + b\gamma^{-1}) - \beta))\} \\
&= \frac{1}{q} \sum_{\gamma \in \mathbb{F}^*_{q^k}} \sum_{c \in \mathbb{F}_q} \chi(c\mathrm{Tr}_{q^k|q}(a\gamma + b\gamma^{-1}) \bar{\chi}(c\beta) \qquad (9) \\
&= \frac{1}{q} \sum_{c \in \mathbb{F}_q} \bar{\chi}(c\beta) \sum_{\gamma \in \mathbb{F}^*_{q^k}} \chi(c\mathrm{Tr}_{q^k|q}(a\gamma + b\gamma^{-1})) \\
&= \frac{1}{q} \sum_{c \in \mathbb{F}_q} \bar{\chi}(c\beta) \sum_{\gamma \in \mathbb{F}^*_{q^k}} \chi^{(k)}(c(a\gamma + b\gamma^{-1})) \\
&= \frac{1}{q} \sum_{c \in \mathbb{F}_q} \bar{\chi}(c\beta) K_k(ca, cb) \\
&= -\frac{1}{q} \sum_{c \in \mathbb{F}_q} \bar{\chi}(c\beta)(\omega_1(ca, cb)^k + \omega_2(ca, cb)^k),
\end{aligned}$$

where the last equation follows from the identities of Kloosterman sums noted earlier, where

$$1 + K_1(a, b)z + qz^2 = (1 - \omega_1(a, b)z)(1 - \omega_2(a, b)z)$$

and $K_1(a, b) = \sum_{\eta \in \mathbb{F}_q} \chi(a\eta + b\eta^{-1})$.

The last part of the theorem could have been obtained using the orthogonality of the characters but the above proof seems more illustrative. 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 Equations 5 and 6.

The following Corollaries emphasize this point of view by emulating multpication 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 Equation (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 Equation (11) is completely analogous.

The following Corollary tries to emulate the recursion relations for the $K_k(a,b)$ of Equation (3).

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

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

PROOF. Although the proof is elementary, using standard transform techniques, we give an outline of it, noting that to use Equation 3 we require $ab\neq 0$:

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

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

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

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

The result of the theorem for the case $s = 1$ is

$$\sum_{\eta\in\mathbb{F}_q}n_{k-1}(\eta,a,b)n_1(\beta-\eta,a,b)+2(q^{k-1}-1).$$

The only other result of a similar nature known to the authors is that in [6] which relates $n_k(\beta)$ to a summation of a certain function over orders in a certain algebraic number field containing the ring of its integers for the case

of $q = 2$ or 3. The generality and simplicity of these Corollaries however is appealing.

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

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

$$n_k(\beta, 0, 0) = \begin{cases} q^k - 1, & \text{if } \beta = 0 \\ 0, & \text{if } \beta \neq 0 \end{cases}$$

$$|n_k(\beta, a, b) - q^{k-1}| \leq 2q^{\frac{k}{2}}, \quad \text{if } ab \neq 0.$$

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 $2q^{\frac{k}{2}}$.

The figures in the following example were used to illustrate and verify many of these Corollaries.

EXAMPLE: To illustrate the above computation, let β be a root of the irreducible polynomial $x^3 + x + 1 \in \mathbb{F}_2[x]$ used to construct $\mathbb{F}_8, q = 8$. We only consider the case $a = b = 1$ and as noted let $K_j(\beta, 1, 1) = K_j(\beta)$ and $n_j(\beta, 1, 1) = n_j(\beta)$. The values for $n_k(\beta)$ were computed directly by computer and the values for $K_j(\beta)$ computed from $K_1(\beta)$ and the recursion (2). The information in the following table is then readily verified:

$\mathbb{F}_q$	0	1	$\{\beta, \beta^2, \beta^4\}$	$\{\beta^3, \beta^5, \beta^6\}$
$tr_{8\|2}$	0	1	0	1
$K_1(\beta)$	7	-5	-1	3
$n_1(\beta)$	1	0	0	2
$K_2(\beta)$	63	-9	15	7
$n_2(\beta)$	15	12	4	8
$K_3(\beta)$	511	-5	23	-45
$n_3(\beta)$	55	90	66	56
$K_4(\beta)$	4095	47	-97	79
$n_4(\beta)$	511	440	520	528
$K_5(\beta)$	32767	275	-281	123
$n_5(\beta)$	4071	3910	4150	4112
$K_6(\beta)$	262143	999	-495	-1001
$n_6(\beta)$	32703	33204	32956	32456

3 Applications of the result

Two simple applications of the results of the previous secion are considered: an interpretation of the set of solutions of an elliptic curve over an extension field in terms of the solutions over the ground field and the enumeration of irreducible polynomials over $\mathbb{F}_q$ whose coefficients satisfy certain condition.

Consider first the set of solutions of an elliptic curve over $\mathbb{F}_{q^k}$ where the equation of the curve is defined over $\mathbb{F}_q$. For this problem we assume fields $\mathbb{F}_q$ and $\mathbb{F}_{q^k}$ of characteristic two only. There are $2(q-1)$ nonisomorphic curves over a field of characteristic two which may be represented by equations of the form

$$y^2 + xy = x^3 + a_2x^2 + a_6, \quad a_2 \in \mathbb{F}_q, \quad a_6 \in \mathbb{F}_q^* \tag{13}$$

where a_2 is chosen to have trace, over $\mathbb{F}_2$, of either 0 or 1. We assume $a_2 = 0$ here. The zeta function for such curve is of the form

$$Z(T) = \frac{P(T)}{(1-T(1-qT)}\ , \quad P(T) = 1 - c_1T + qT^2 = (1-\omega_1T)(1-\bar{\omega_1}T)$$

where the number of points of Equation (13) is $\#E(\mathbb{F}_q) = q+1-c_1$. It is easy

to see that

$$\#E(\mathbb{F}_{q^k}) = q^k + 1 - c_k = q^k + 1 - {\omega_1}^k - {\bar{\omega_1}}^k$$

where the c_i satisfy the recursion $c_n = c_1 c_{n-1} - q c_{n-2},\ c_0 = 2$. The relationship between these facts and the corresponding Kloosterman sums is immediate.

We wish to make an elementary observation on these facts by using the results of the previous section. Consider the Equation (13) with $a_2 = 0$. Transform the equation by letting $y = xz,\ x \neq 0$ and set $x = \sqrt[4]{a_6}u$ (squaring in a field of characteristic 2 is an isomporphism) to give the equation:

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

The equation will have two distinct solutions iff

$$Tr_{q^k|2}(\sqrt[4]{u + u^{-1}}) = 0. \tag{14}$$

and the total number of solutions will be $0 \pmod 4$. From the previous section we have that

$$S_k(\beta, 1, 1) = S_k(\beta) = \{\gamma \in \mathbb{F}_{q^k} | Tr_{q^k|q}(\gamma + \gamma^{-1}) = \beta\}$$

and $|S_k(\beta)| = n_k(\beta, 1, 1) = n_k(\beta)$. Now the trace of Equation (14) can be realized in two steps, first $Tr_{q^k|q}$ and then $Tr_{q|2}$. Thus if we define

$$T_0 = \{\alpha \in \mathbb{F}_q \mid Tr_{q|2}(a\alpha) = 0\}\ ,\quad a = \sqrt{a_6}.$$

It follows immediately from the transitivity of the trace function that

$$\#E(\mathbb{F}_{q^k}) = \sum_{\beta \in T_0} n_k(\beta).$$

In words we have that the number of solutions of the Equation (13) ($a_2 = 0$) is determined entirely by the quantities $n_k(\beta)$ and the set T_0 and the only effect of the constant a_6 is to determine the set T_0. This gives a direct observation of how the number of points on the curve of Equation (13) over $\mathbb{F}_q$ determines the number of points of the curve over $\mathbb{F}_{q^k}$.

The second application concerns the enumeration of certain irreducible polynomials over $\mathbb{F}_q$. The enumeration of irreducible polynomials such that certain coefficients are chosen independently has been of great interest in receent literature (see [4] for a recent sumary of 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

$$X^k + c_1 X^{k-1} + \cdots + c_{k-1}X + c_k \in \mathbb{F}_q[X]$$

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 cefficients 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 polynoials 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

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

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

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

which is equivalent to

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

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,

$$\left| I_{q,k}(0) - \frac{q^{k-1}}{k} \right| \leq \frac{1}{kq} \left(1 + \sum_{\substack{d|k \\ d<k}} (q^d - 1) + (q-1) \sum_{d|k} 2q^{\frac{d}{2}} \right)$$
$$\leq \frac{1}{kq} \left(q \frac{q^{\frac{k}{2}} - 1}{q-1} + 2(q-1) \frac{q^{\frac{k}{2}+1} - q^{\frac{1}{2}}}{q-1} \right)$$
$$\leq \frac{q^{\frac{k}{2}}}{kq} \frac{2q^2 - q}{q-1}$$
$$\leq \frac{3q^{\frac{k}{2}}}{k}.$$

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 $f = X^k + c_1 X^{k-1} + \cdots + c_{k-1} X + c_k \in \mathbb{F}_q[X]$, 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

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

Since we are in a field of characteristic 2 or 3, and $(\frac{k}{d}, q) = 1$, 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

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

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.

4 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, in similarity to the Kloosterman sums themselves. These quantities are used to give a direct interpretation of the number of points over $\mathbb{F}_{q^k}$ of an elliptic curve, defined over $\mathbb{F}_q$. Additionally the result was related to determining the number of irreducible polynomials over $\mathbb{F}_q$ that satisfy a certain condition on certain of its coefficients.

ACKNOWLEDGEMENT: The authors would like to thank Chris Studholme for obtaining the figures in the example of Section 2, using NTL.

References

[1] I.F. Blake, G. Seroussi and N. Smart. *Elliptic Curves in Cryptography.* Cambridge University Press, Lecture Note Series vol. 265, 1999.

[2] I.F. Blake, G. Seroussi and Ron Roth. On the solutions of an elliptic curve over a field of characteristic two. *Proceedings Int'l. Symp. Information Theory, Cambridge, MA 1998.*

[3] L. Carlitz. Kloosterman sums and finite field extensions. *Acta Aritmetica* vol. XVI, pp. 1799-193, 1969.

[4] Stephen D. Cohen. Explicit theorems on generator polynomials. *Finite Fields and their Applications.* vol. 11, pp. 337-357, 2005.

[5] Tor Helleseth and Victor Zinoviev. On a new identity for Kloosterman sums and nonlinear system of equations over finite fields of characteristic 2. *Discrete Mathematics.* vol. 274, pp. 109-124, 2004.

[6] Nicholas Katz and Ron Livné. Sommes Kloosterman et courbes elliptiques universelles en caractéristiques 2 et 3. C.R. Acad. Sci. Paris. vol. 309, Série I, pp. 723-726, 1989.

[7] Gilles Lachaud et Jacques Wolfmann. Sommes de Kloosterman, courbes elliptiques et codes cycliques en caractéristique 2. C.R. Acad. Sci. Paris. vol. 305, Série I, pp. 881-883, 1987.

[8] H. Niederreiter. An emumeration formula for certain irreducible polynomials with an application to the construction of irreducaible polynomials over the binary field. *AAECC* vol. 1, pp. 119-124, 1990.

[9] H. Niederreiter and R. Lidl. *Finite Fields*. Cambridge, UK: Cambridge University Press, 2nd Edition, 1997.

[10] Dong-Joon Shin and Wonjin Sung. A new Kloosterman sum identity over $\mathbb{F}_{2^m}$ for odd m. *Discrete Mathematics*. vol. 268, pp. 337-341, 2003.

[11] Joseph L. Yucas and Gary L. Mullen. Irreducible polynomials over GF(2) with prescribed coefficients. *Discrete Mathematics*. vol. 274, pp. 265-279, 2004.