

# A note on Kloosterman sums and its application

Ian F. Blake

Department of Electrical and Computer Engineering  
University of Toronto  
Email: ifblake@comm.toronto.edu

Theo Garefalakis

Department of Mathematics  
University of Crete  
Email: theo@math.uoc.gr

**Abstract**—The number of times the trace of a certain function on an extension field assumes a fixed value in the base field is considered. It is shown that the set of all such values enjoys a Fourier transform like property with Kloosterman sums. The application of this property to coding and cryptography is briefly discussed.

## I. 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  $\chi$  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 [10] 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

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

for some fixed element  $a \in \mathbb{F}_q$  where  $\text{Tr}_{q|p}$  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 nontrivial 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 [10], as well as the original work of Carlitz [3] which established many of the properties which are extended here.

Characters satisfy the orthogonality relations:

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

where  $\delta_{ab}$  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

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

The sums

$$K_1(a, b) = K(a, b) = \sum_{\alpha \in \mathbb{F}_q^*} \chi(a\alpha + b\alpha^{-1})$$

and

$$K_k(a, b) = \sum_{\gamma \in \mathbb{F}_{q^k}^*} \chi^{(k)}(a\gamma + b\gamma^{-1})$$

for  $a, b$  fixed elements of  $\mathbb{F}_q$ , are referred to as Kloosterman sums [10]. 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.

Kloosterman sums have been widely investigated and satisfy many interesting relations. A fundamental result is that

$$K_k(a, b) = -\omega_1^k(a, b) - \omega_2^k(a, b) \quad (1)$$

where  $\omega_1(a, b), \omega_2(a, b)$  (or simply  $\omega_1$  and  $\omega_2$  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], [10]:

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

More generally, by the same argument, we have:

$$\begin{aligned} K_k(a, b) &= -K_s(a, b)K_{k-s}(a, b) - q^s K_{k-2s}(a, b) \\ k \geq 2, \quad K_0(a, b) &= -2, \quad ab \neq 0, \quad 1 \leq s \leq \lfloor k/2 \rfloor \end{aligned}$$

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  $K_k(0, 0) = K_k(0) = q^k - 1$ .

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], [8], [11]). 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 [7], which gives results for the case  $q = 2$  and  $3$ . Such numbers will be shown to have a Fourier transform type of relation with the Kloosterman sums themselves. However these numbers tend to be of more interest in applications than the Kloosterman sums themselves. While the results are simple to prove and follow quite directly from definitions, this approach seems novel and useful.

$\text{Tr}_{q^k|q}(\cdot)$  is the trace function of  $\mathbb{F}_{q^k}$  over  $\mathbb{F}_q$ . A few easy observations are recorded below (where  $q$  is understood).

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

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

The following theorem gives the fundamental relationship between these numbers and Kloosterman sums. The proofs will be omitted here.

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

$$\begin{aligned} K_k(ca, cb) &= \sum_{\eta \in \mathbb{F}_q} n_k(\eta, a, b) \chi(c\eta) \\ \Leftrightarrow n_k(\beta, a, b) &= \frac{1}{q} \sum_{c \in \mathbb{F}_q} \bar{\chi}(c\beta) K_k(ca, cb) \end{aligned} \quad (4)$$

It is emphasized that the 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 the above Theorem. Furthermore, both sets of quantities are entirely determined by their values for  $k = 1$  via recursions mentioned for Kloosterman sums earlier and shown below for the parameters  $n_k$ .

Several instances of the relation between the two sets of parameters are given below. The proofs are straightforward, emulating the usual Fourier transform type of proofs between multiplication and convolution in the two domains. The proofs are omitted here.

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

$$\frac{1}{q} \sum_{c \in \mathbb{F}_q} \bar{\chi}(c\beta) K_k^2(ca, cb) = \sum_{\eta \in \mathbb{F}_q} n_k(\eta, a, b) n_k(\beta - \eta, a, b) \quad (5)$$

$$\sum_{\beta \in \mathbb{F}_q} \chi(c\beta) n_k^2(\beta, a, b) = \frac{1}{q} \sum_{d \in \mathbb{F}_q} K_k(da, db) \cdot \quad (6)$$

$$K_k((c-d)a, (c-d)b). \quad (7)$$

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

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

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

The generality and simplicity of these Corollaries 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  $|n_k(\beta, a, b) - q^{k-1}| \leq 2q^{\frac{k}{2}}$ , if  $ab \neq 0$  and

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

Thus the known bounds on Kloosterman sums translate into a uniformity property of the sets  $\{n_k(\beta, a, a)\}$ . There are many more identities between the  $n_k$  values and the Kloosterman sums that can be obtained but the above give the sense of the relations that are possible and useful.

## II. 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.

One of the original motivations for this work was to determine a more explicit understanding of the Riemann zeta function for elliptic curves i.e. to show how the numbers of solutions of an elliptic curve over a base finite field  $\mathbb{F}_q$  completely determines the number of solutions over an extension field  $\mathbb{F}_{q^k}$ . The question was considered in an earlier work [2] but taken much further here. It has been shown that a similar statement holds for the the  $n_k$  quantities as well. It might be noted that relationship between the numbers of points on elliptic curves over finite fields of characteristic two was discussed in the work of Lachaud and Wolfman [8]; indeed the Frobenius trace of the curve is in fact a Kloosterman sum. The interest here was to consider the values over extension fields.

Another use of the relations found here is in determining the complete weight enumerator of Melas codes [6] The results can also be related to determining the number of irreducible polynomials over  $\mathbb{F}_q$  that satisfy a certain condition on certain of its coefficients. These interesting problems will be pursued in the final version of the paper.

## 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 Arithmetica* vol. XVI, pp. 179-193, 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] Toyokazu Hiramatsu and Günter Köhler. *Coding Theory and Number Theory*. Kluwer Academic Publishers. 2003.
- [7] 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.

- [8] 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.
- [9] H. Niederreiter. An enumeration formula for certain irreducible polynomials with an application to the construction of irreducible polynomials over the binary field. *AAECC* vol. 1, pp. 119-124, 1990.
- [10] H. Niederreiter and R. Lidl. *Finite Fields*. Cambridge, UK: Cambridge University Press, 2nd Edition, 1997.
- [11] 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.
- [12] Joseph L. Yucas and Gary L. Mullen. Irreducible polynomials over  $\text{GF}(2)$  with prescribed coefficients. *Discrete Mathematics.* vol. 274, pp. 265-279, 2004.