

On zeros of Kloosterman sums

Petr Lisoněk
Simon Fraser University

The Mathematical Interests of Peter Borwein
15 May 2008

- 1 Background
- 2 Motivation
- 3 Divisibility Results
- 4 Values on Subfields

Finite fields

$$q = p^m, p \in \{2, 3\}, m \in \mathbb{N}$$

$$\omega_p = e^{2\pi i/p}$$

$$\mathbb{F}_q = \text{GF}(q)$$

$$\text{Tr} : \mathbb{F}_q \rightarrow \mathbb{F}_p, \quad \text{Tr}(a) := \sum_{j=0}^{m-1} a^{p^j} \quad \text{absolute trace}$$

Definition

$$q = p^m$$

The **Kloosterman sum** $\mathcal{K}_q : \mathbb{F}_q \rightarrow \mathbb{R}$ is defined by

$$\mathcal{K}_q(a) := 1 + \sum_{x \in \mathbb{F}_q^*} \omega_p^{\text{Tr}(x^{-1}+ax)},$$

or equivalently

$$\mathcal{K}_q(a) := \sum_{x \in \mathbb{F}_q} \omega_p^{\text{Tr}(x^{-1}+ax)},$$

if we let $\text{Tr}(0^{-1}) = 0$.

Note that $\mathcal{K}_{p^m}(a) = \mathcal{K}_{p^m}(a^p)$.

Zeros of \mathcal{K}_q

$$\mathcal{K}_q(0) = 0$$

We say that $a \in \mathbb{F}_q$ is a **zero of the Kloosterman sum** if $\mathcal{K}_q(a) = 0$.

Relation to elliptic curves

Theorem. (Lachaud and Wolfmann, 1990)

For $a \in \mathbb{F}_{2^m}^*$ let $\mathcal{E}_{2^m}(a)$ be the elliptic curve over \mathbb{F}_{2^m} defined by

$$\mathcal{E}_{2^m}(a) : y^2 + xy = x^3 + a.$$

Then $\#\mathcal{E}_{2^m}(a) = 2^m + \mathcal{K}_{2^m}(a)$.

Theorem. (Moisio 2007, to appear in *Acta Arithmetica*)

For $a \in \mathbb{F}_{3^m}^*$ let $\mathcal{E}_{3^m}(a)$ be the elliptic curve over \mathbb{F}_{3^m} defined by

$$\mathcal{E}_{3^m}(a) : y^2 = x^3 + x^2 - a.$$

Then $\#\mathcal{E}_{3^m}(a) = 3^m + \mathcal{K}_{3^m}(a)$.

Range of \mathcal{K}_q

Theorem. (Lachaud and Wolfmann, 1990)

$$\{\mathcal{K}_{2^m}(a) : a \in \mathbb{F}_{2^m}\} = \{k : k \equiv 0 \pmod{4}, k \in (-2^{m/2+1}, 2^{m/2+1})\}$$

Theorem. (Katz 1989, Moisisio 2007)

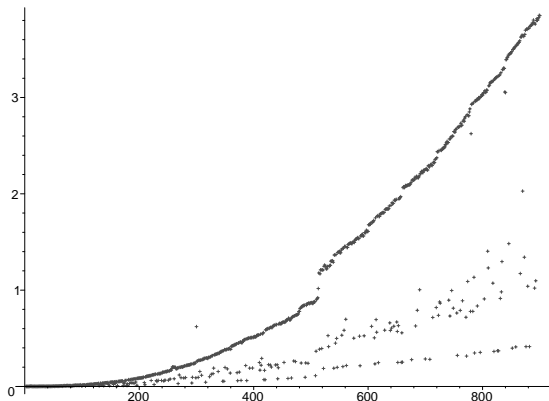
$$\{\mathcal{K}_{3^m}(a) : a \in \mathbb{F}_{3^m}\} = \{k : k \equiv 0 \pmod{3}, k \in (-2 \cdot 3^{m/2}, 2 \cdot 3^{m/2})\}$$

Applications of the $\mathcal{K}_q(a) \leftrightarrow \mathcal{E}_q(a)$ correspondence

- 1 proof techniques
- 2 explicit computation of $\mathcal{K}_q(a)$ (SEA algorithm etc.)

Time (in seconds) to evaluate a random $\mathcal{K}_{2^m}(a)$, $m \leq 900$

Magma 2.14, Intel Xeon CPU at 3.0 GHz, 4 MB cache



Symmetric (private key) encryption

DES (1977), AES (2000)

Encryption/decryption consists of ~ 16 rounds of:

- (1) adding a round key
- (2) permutation
- (3) substitution (S-box)

Only part (3), the S-boxes, introduce non-linearity into the process.

differential cryptanalysis, linear cryptanalysis

DES S-boxes $\mathbb{F}_2^6 \rightarrow \mathbb{F}_2^4$ have never been explained.

AES S-box is based on $\mathbb{F}_{2^8} \rightarrow \mathbb{F}_{2^8}$, $x \mapsto x^{-1}$.

Highly non-linear functions

$\mathcal{K}_{2^m}(a) = \sum_x (-1)^{\text{Tr}(ax+x^{-1})}$ measures the correlation between the linear function $\text{Tr}(ax)$ and the function $\text{Tr}(x^{-1})$.

(almost) bent functions - Dillon (1974) $\mathcal{K}_{2^m}(a) = 0$

Finite geometries, linear codes, design of experiments

caps with many free pairs of points

L. (*J. Comb. Des.* 2006)

Garaschuk & L. (*Des. Codes Crypt.* 2008)

One option for showing $\mathcal{K}_q(a) \neq 0$

$$n \nmid \mathcal{K}_q(a) \implies \mathcal{K}_q(a) \neq 0$$

Divisibility of $\mathcal{K}(a)$ and point orders

Theorem

Let $p \in \{2, 3\}$, and let $1 \leq k \leq m$. Then $p^k | \mathcal{K}_{p^m}(a)$ if and only if there exists a point of order p^k on $\mathcal{E}_{p^m}(a)$, where the curves \mathcal{E}_{p^m} were defined earlier.

Proof. By theorems of Lachaud & Wolfmann and Moisisio we have that $p^k | \mathcal{K}_{p^m}(a)$ if and only if $p^k | \#\mathcal{E}_{p^m}(a)$. Recall the Abelian structure $\mathcal{E}_{p^m}(a) \simeq \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$, with $n_1 | n_2$ and $n_1 | p^m - 1$; we have $\#\mathcal{E}_{p^m}(a) = n_1 n_2$. Suppose that $p^k | \#\mathcal{E}_{p^m}(a)$. Since $p \nmid n_1$, it follows that $p^k | n_2$ and $\mathcal{E}_{p^m}(a)$ contains a subgroup G isomorphic to \mathbb{Z}_{p^k} . A generator of G is a point of order p^k in $\mathcal{E}_{p^m}(a)$. Conversely, if $\mathcal{E}_{p^m}(a)$ contains a point of order p^k , then $p^k | \#\mathcal{E}_{p^m}(a)$ by the Lagrange Theorem.

$8|\mathcal{K}_{2^m}(a)$

Helleseth & Zinoviev (1999), system of polynomial equations

Theorem

$\mathcal{K}_{2^m}(a)$ is divisible by 8 if and only if $\text{Tr}(a) = 0$.

Shorter **proof**:

We have $8|\mathcal{K}_{2^m}(a)$ if and only if $\mathcal{E}_{2^m}(a)$ contains a point of order 8; for simplicity we can take the curve $\mathcal{E}_{2^m}(a^8)$. Using theory of *division polynomials*, an $x_0 \in \mathbb{F}_{2^m}$ is the x -coordinate of a point of order 8 on $\mathcal{E}_{2^m}(a^8)$ if and only if $X = x_0$ is a root of the polynomial $(X + a^2)^2 + aX$. This happens exactly if $\text{Tr}(1 \cdot a^4/a^2) = \text{Tr}(a) = 0$.

$16 \mid \mathcal{K}_{2^m}(a)$

Theorem

$\mathcal{K}_{2^m}(a)$ is divisible by 16 if and only if $\text{Tr}(a) = 0$ and $\text{Tr}(y) = 0$ where $y^2 + ay + a^3 = 0$.

Proof. division polynomials, solvability of quartics over \mathbb{F}_{2^m}

A ternary analogue

Theorem

$\mathcal{K}_{3^m}(a)$ is divisible by 9 if and only if $\text{Tr}(a) = 0$.

Finding/proving zeros of \mathcal{K}_q

Numerical examples of zeros of Kloosterman sums found in the literature are typically limited to very small field orders.

In order to **prove** that $\mathcal{K}(a) = 0$ for some given $a \in \mathbb{F}_{p^m}$ ($p \in \{2, 3\}$), one does not need to use point counting. In this case the group of the elliptic curve must be isomorphic to \mathbb{Z}_{p^m} , and one can simply attempt to guess a generator P for the group. (The probability of success is $1 - 1/p$ per one guess.) If P indeed happens to be a generator, then this can be easily verified by computing $p^i P$ for $i = 1, 2, \dots, m$; this can be further simplified using the division polynomials.

Starting with random elements $a \in \mathbb{F}_{p^m}$, in just a few CPU days we found a non-trivial Kloosterman zero for each field \mathbb{F}_{2^m} where $m \leq 64$ and for each field \mathbb{F}_{3^m} where $m \leq 34$.

P. Charpin, G. Gong, Hyperbent functions, Kloosterman sums and Dickson polynomials. Technical report CACR 2007-29, Centre for Applied Cryptographic Research (CACR), University of Waterloo, 2007. (25 pages)

<http://www.cacr.math.uwaterloo.ca/>

Theorem

We have $\mathcal{K}_{2^m}(1) \neq 0$ unless $m = 4$.

A short proof of $m \neq 4 \Rightarrow \mathcal{K}_{2^m}(1) \neq 0$

Recall $\mathcal{K}_{2^m}(1) = \#\mathcal{E}_{2^m}(1) - 2^m$ where $\mathcal{E}_{2^m}(1) : y^2 + xy = x^3 + 1$.

Consider $\mathcal{E}_{2^m}(1)$ over \mathbb{F}_2 and apply the Hasse-Weil Theorem:

$$\zeta(\mathcal{E}_{2^m}(1)) = \frac{2T^2 + T + 1}{(1 - T)(1 - 2T)}$$

An easy calculation shows that $k_m := \mathcal{K}_{2^m}(1)$ satisfies

$k_{m+3} = -k_{m+1} + 2k_m$, hence

$$k_m \bmod 96 = 2, 4, -4, 0, \overline{[12, -8, -12, 32, -4, 40, -28, 48]}.$$

Zeros in subfields

Conjecture.

Suppose that \mathbb{F}_{2^k} is a proper subfield of \mathbb{F}_{2^m} , $m > 4$. If $\mathcal{K}_{2^m}(a) = 0$ and $a \in \mathbb{F}_{2^k}$, then $a = 0$.

previous slide: proof for $k = 1$

numerical evidence