Kloosterman Zeros and Vectorial Bent Functions

Petr Lisoněk
Simon Fraser University
Burnaby, BC, Canada

Boolean Functions and their Applications
(BFA 2019)

18 June 2019
Florence, Italy

Outline

1. Identities for Kloosterman sums
2. Listing Kloosterman zeros
3. Triple Kloosterman zero (TKZ) vectorial bent functions
4. Non-existence of Dillon-type vectorial bent functions

Definitions

For $m|n$ we define the trace function $\mathrm{Tr}_m^n : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ by

$$\mathrm{Tr}_m^n(x) = \sum_{i=0}^{n/m-1} x^{2^{im}}.$$

The *Kloosterman sum* is the mapping $\mathcal{K} : \mathbb{F}_{2^m} \to \mathbb{Z}$ defined by

$$\mathcal{K}(a) = 1 + \sum_{x \in \mathbb{F}_{2^m}^*} (-1)^{\mathrm{Tr}(x^{-1}+ax)}.$$

An a such that $\mathcal{K}(a) = 0$ is called a Kloosterman zero.

Theorem (Dillon 1976; Helleseth-Kholosha 2006)

Let $p \in \{2, 3\}$ and $a \in \mathbb{F}_{p^{n/2}}^*$. Then $f(x) = \mathrm{Tr}_1^n(ax^{p^{n/2}-1})$ is (hyper-)bent if and only if $\mathcal{K}_{p^{n/2}}(a) = 0$.

Elliptic curves and Kloosterman sums

Theorem (Lachaud & Wolfmann 1987)

For $a \in \mathbb{F}_{2^m}^*$

$$\#E_2^a(\mathbb{F}_{2^m}) = 2^m + \mathcal{K}_{2^m}(a)$$

where $E_2^a : y^2 + xy = x^3 + a$.

Theorem (Katz & Livné 1989)

For $a \in \mathbb{F}_{3^m}^*$

$$\#E_3^a(\mathbb{F}_{3^m}) = 3^m + \mathcal{K}_{3^m}(a)$$

where $E_3^a : y^2 = x^3 + x^2 - a$.

Identities for Kloosterman sums

There has been a lot of interest in *identities* for Kloosterman sums of the form $\mathcal{K}(f(a,\ldots)) = \mathcal{K}(g(a,\ldots))$ where f and g are rational functions of 1 or more variables.

Most recent preprint:
Minglong Qi, Shengwu Xiong, New Kloosterman sum identities from the Helleseth-Zinoviev result on $\mathbb{Z}_4$-linear Goethals codes. arXiv:1904.07330 (April 2019)

But are they really new?

Identities for Kloosterman sums (cont'd)

P. Lisoněk, Identities for Kloosterman sums and modular curves. Contemporary Mathematics 524 (2012), 125–130. (Proceedings of AGCT 2011)

— uses the known connection of Kloosterman sums and elliptic curves to provide a general framework for proving Kloosterman sum identities.

Let $\Phi_\ell(X, Y)$ be the *classical modular polynomial of level* ℓ (modular equation for j of order ℓ).

Identities for Kloosterman sums (cont'd)

Theorem (Kojo 2002)

For $a, b \in \mathbb{F}_{2^m}^*$ we have $\mathcal{K}(a) = \mathcal{K}(b)$ if and only if there exists $\ell \in \mathbb{N}$ such that $\Phi_\ell(a^{-1}, b^{-1}) = 0$.

Theorem (L. 2012)

For $a, b \in \mathbb{F}_{3^m}^*$ we have $\mathcal{K}(a) = \mathcal{K}(b)$ if and only if there exists $\ell \in \mathbb{N}$ such that $\Phi_\ell(a^{-1}, b^{-1}) = 0$.

Identities for Kloosterman sums (cont'd)

This allows for *very simple* proofs of identities, that *only* amount to checking that a certain rational function vanishes identically. The proofs are easily executed in a computer algebra system (e.g., Magma).

This method also allows for detection of *algebraic dependence* between identities previously thought to be independent.

In characteristic 2 all following identities had been previously known.

Identities for Kloosterman sums (cont'd) char 2

Theorem

Let $b \in \mathbb{F}_{2^m}$. We have:

(a)
$$\mathcal{K}\left(b^3(1+b)\right) = \mathcal{K}\left(b(1+b)^3\right)$$

(b)
$$\mathcal{K}\left(b^5(1+b)\right) = \mathcal{K}\left(b(1+b)^5\right)$$

(c) *If $b^2+b+1 \neq 0$, then*
$$\mathcal{K}\left(\frac{b^7(1+b)}{(b^2+b+1)^4}\right) = \mathcal{K}\left(\frac{b(1+b)^7}{(b^2+b+1)^4}\right).$$

(d) *If $b^2+b+1 \neq 0$, then*
$$\mathcal{K}\left(\frac{b^{13}(1+b)}{(b^2+b+1)^4}\right) = \mathcal{K}\left(\frac{b(1+b)^{13}}{(b^2+b+1)^4}\right).$$

Identities for Kloosterman sums (cont'd) char 3

Theorem (L. 2012)

Let $b \in \mathbb{F}_{3^m}$. We have:

(a)
$$\mathcal{K}\left(b^2(1-b)\right) = \mathcal{K}\left(b(1-b)^2\right)$$

(b) *If $b^2+b-1 \neq 0$, then*
$$\mathcal{K}\left(\frac{b^5(b-1)}{(b^2+b-1)^3}\right) = \mathcal{K}\left(\frac{b(b-1)^5}{(b^2+b-1)^3}\right).$$

(c) *If $b \neq -1$, then*
$$\mathcal{K}\left(\frac{b^7(1-b)}{(b+1)^2}\right) = \mathcal{K}\left(\frac{b(1-b)^7}{(b+1)^2}\right).$$

(d) *If $b \neq -1$ and $b^2-b-1 \neq 0$, then*

Back to Qi & Xiong

Minglong Qi, Shengwu Xiong, New Kloosterman sum identities from the Helleseth-Zinoviev result on $\mathbb{Z}_4$-linear Goethals codes. arXiv:1904.07330 (April 2019)

— All their "new" multivariate identities are algebraically equivalent to the Helleseth-Zinoviev identity (first entry in the list for char 2). This can be *easily* determined by the method explained on the previous slides.

Listing Kloosterman zeros exhaustively

Previously in the literature Kloosterman zeros were exhaustively listed only for fields of orders up to 2^{14}. With our new method we are able to list all Kloosterman zeros in all binary fields of order up to 2^{63} in a few days of CPU time.

Recall

Theorem (Kojo 2002)

For $a, b \in \mathbb{F}_{2^m}^*$ we have $\mathcal{K}(a) = \mathcal{K}(b)$ if and only if there exists $\ell \in \mathbb{N}$ such that $\Phi_\ell(a^{-1}, b^{-1}) = 0$.

Listing Kloosterman zeros exhaustively

Algorithm for listing all Kloosterman zeros in $\mathbb{F}_{2^m}$ (L.)

1. Find one Kloosterman zero in $\mathbb{F}_{2^m}$. For this use (L. SETA 2008) or (Ahmadi & Granger, Math.Comp. 2014).
2. Iterate Kojo's theorem, with increasing ℓ whenever needed. (moderate levels are enough for $m \leq 62$.)
3. Stopping condition: The number of Kloosterman zeros is given by a certain *Kronecker class number*, which is easy to compute (follows from Schoof 1987).

Step 2 only requires finding roots in $\mathbb{F}_{2^m}$ of univariate polynomials over $\mathbb{F}_{2^m}$.

Vectorial bent functions

Definition

For $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ and $a \in \mathbb{F}_{2^m}^*$ we define the *component function* $f_a(x) = \mathrm{Tr}_1^m(af(x))$.

Definition

Function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is *vectorial bent* if all its component functions are bent.

Equivalently, a vectorial bent function mapping to $\mathbb{F}_{2^m}$ is an m-dimensional vector space of bent functions mapping to $\mathbb{F}_2$.

Triple Kloosterman zero (TKZ) vectorial bent functions

We introduce a new class of vectorial bent functions from $\mathbb{F}_{2^{2m}}$ to $\mathbb{F}_4$.

Definition

Let $a_1, a_2, a_3 \in \mathbb{F}_{2^m}^*$ be Kloosterman zeros such that $a_1 + a_2 + a_3 = 0$. Let $F_c(x) = \mathrm{Tr}_1^{2m}(cx^{2^m-1})$ and $\mathbb{F}_4 = \mathbb{F}_2(\omega)$. Then $f(x) = F_{a_1}(x) + \omega F_{a_2}(x)$ is a vectorial bent function from $\mathbb{F}_{2^{2m}}$ to $\mathbb{F}_4$, called *triple Kloosterman zero (TKZ) function.*

Most binary fields on which we performed computations contain *many* triples of Kloosterman zeros adding to 0, hence TKZ vectorial bent functions exist for them.

Non-existence results

We further examine bentness of the Dillon-type monomial functions $f(x) = \mathrm{Tr}_m^n(ax^{2^{n/2}-1})$, now in the vectorial case $m > 1$. Without loss of generality we can assume $a \in \mathbb{F}_{2^{n/2}}$.

Theorem (Muratović-Ribić & Pasalic & Bajrić 2014)

There are no bent functions of the form $f(x) = \mathrm{Tr}_m^{2m}(ax^{2^m-1})$ where $a \in \mathbb{F}_{2^m}$.

Theorem (Lapierre, L. 2016)

Let m be even and let $a \in \mathbb{F}_{2^m}^*$. The function $f(x) = \mathrm{Tr}_{m/2}^{2m}(ax^{2^m-1})$ is not bent.

We now look at the functions from $\mathbb{F}_{2^{2m}}$ to $\mathbb{F}_{2^{m/3}}$. This section is joint work with Lucien Lapierre.

Non-existence results

From now on let $\mathcal{T}_{2^t}(a)$ denote the absolute trace of a.

Further we define the *subtrace* of a by

$$\mathcal{S}_{2^t}(a) = \sum_{0 \le i < j < t} a^{2^i + 2^j}.$$

Proposition

Assume that $m \ge 4$ and $a \in \mathbb{F}_{2^m}^*$. If $\mathcal{K}_{2^m}(a)$ is divisible by 16, then $\mathcal{T}_{2^m}(a) = 0$ and $\mathcal{S}_{2^m}(a) = 0$.

Non-existence results

Proposition

Let $a \in \mathbb{F}_{2^m}^*$ and suppose that k divides m. Then $f(x) = \mathrm{Tr}_k^{2m}(ax^{2^m-1})$ is bent if and only if $\mathcal{K}_{2^m}(u) = 0$ for all $u \in a\mathbb{F}_{2^k}^*$.

Theorem

Assume that k is odd, *$k \geq 3$, and denote $m = 3k$. Assume that $a \in \mathbb{F}_{2^{2m}}^*$. Then $f(x) = \mathrm{Tr}_k^{2m}(ax^{2^m-1})$ is not bent.*

Non-existence results

Sketch of proof:
TAC assume the function is bent, then

$$\mathcal{T}_{2^m}(az) = \mathcal{S}_{2^m}(az) = 0 \quad \text{for each } z \in \mathbb{F}_{2^k}.$$

We express these conditions as a system of bivariate polynomial equations and by polynomial elimination methods combined with using the finite field structure we conclude $a \in \mathbb{F}_{2^k}$. This implies $\mathcal{K}(a) = 0$, which is a contradiction to (L., Moisio 2011).

In the case k even the same methods yield a slightly weaker result, since indeed examples of such bent functions with $2m = 12$ variables do exist.

Non-existence results

Theorem

Assume that k is even *and denote $m = 3k$. If $f(x) = \mathrm{Tr}_k^{2m}(ax^{2^m-1})$ is bent, then $a^{3(2^k-1)} + 1 = 0$.*

Example: Let $k = 2$, then $a^9 + 1 = 0$. If a is any of the primitive 9-th roots of unity in $\mathbb{F}_{2^6}$, then $f(x) = \mathrm{Tr}_2^{12}(ax^{2^6-1})$ is bent.

Outlook

In the part on non-existence results we used properties of the second and the third coefficient of the characteristic polynomial of a Kloosterman zero: its trace and its subtrace. We introduced new polynomial elimination methods to obtain algebraic conditions for the putative bent function coefficient.

Results in
F. Göloğlu, P. Lisoněk, G. McGuire, R. Moloney,
Binary Kloosterman sums modulo 256 and coefficients of the characteristic polynomial. IEEE Trans. Inform. Theory (2012)
might be possibly used to derive further stronger results.