Binary and Ternary Kloosterman sums

Kseniya Garaschuk

University of Victoria

July 22, 2010

The trace mapping

$\mathbb{F}_{p^m}$ ... finite field of order p^m, p is prime
$\mathbb{F}^*_{p^m} := \mathbb{F}_{p^m} \setminus \{0\}$

$\mathrm{Tr} : \mathbb{F}_{p^m} \rightarrow \mathbb{F}_p$ ... trace mapping given by:

$$\mathrm{Tr}(x) = \sum_{i=0}^{m-1} x^{p^i} = x + x^p + \cdots + x^{p^{m-1}}.$$

General Kloosterman map

Definition

The Kloosterman map is the mapping $K : \mathbb{F}_{p^m} \to \mathbb{R}$ defined by

$$K(a) := \sum_{x \in \mathbb{F}_{p^m}^*} \omega^{\mathrm{Tr}(x^{-1}+ax)},$$

where $\omega = e^{2\pi i/p}$.

Spectrum of binary Kloosterman sums

$\Uparrow$

(Lachaud and Wolfmann)

$\Downarrow$

Number of points on elliptic curves

General Kloosterman map

Definition

The Kloosterman map is the mapping $K : \mathbb{F}_{p^m} \longrightarrow \mathbb{R}$ defined by

$$K(a) := \sum_{x \in \mathbb{F}_{p^m}^*} \omega^{\mathrm{Tr}(x^{-1}+ax)},$$

where $\omega = e^{2\pi i/p}$.

Spectrum of binary Kloosterman sums

$\Uparrow$

(Lachaud and Wolfmann)

$\Downarrow$

Number of points on elliptic curves

Binary Kloosterman curves

Theorem (Lachaud, Wolfmann)

An ordinary elliptic curve $\mathcal{E}$ over $\mathbb{F}_{2^m}$ can be transformed into one of the Kloosterman curves:

$$\mathcal{K}_a^+ : y^2 + y = ax + \frac{1}{x},$$
$$\mathcal{K}_a^- : y^2 + y = ax + \frac{1}{x} + \tau,$$

where $a, \tau \in \mathbb{F}_{2^m}$, $\mathrm{Tr}(\tau) = 1$.

Theorem (Lachaud, Wolfmann)

Let $a \in \mathbb{F}_{2^m}$. Then $\#\mathcal{K}_a^{\pm} = 2^m + 1 \pm K(a)$.

Applications of Kloosterman sums: cross-correlation functions

- Consider two binary sequences with period $2^m - 1$, $u(t) = \mathrm{Tr}(\alpha^t)$ and $v(t) = u(-t)$.
- The cross-correlation function between $u(t)$ and $v(t)$ is defined by

$$C_t(a) = \sum_{t=0}^{2^m-2} (-1)^{u(t+a)+v(t)} = \sum_{x \in \mathbb{F}_{2^m}^*} (-1)^{\mathrm{Tr}(x^{-1}+ax)} = K(a).$$

- Problem: determine the values and the number of occurrences of each value taken on by $C_t(a)$.

Applications of Kloosterman sums: cross-correlation functions

- Consider two binary sequences with period $2^m - 1$, $u(t) = \mathrm{Tr}(\alpha^t)$ and $v(t) = u(-t)$.
- The cross-correlation function between $u(t)$ and $v(t)$ is defined by

$$C_t(a) = \sum_{t=0}^{2^m-2} (-1)^{u(t+a)+v(t)} = \sum_{x \in \mathbb{F}_{2^m}^*} (-1)^{\mathrm{Tr}(x^{-1}+ax)} = K(a).$$

- Problem: determine the values and the number of occurrences of each value taken on by $C_t(a)$.

Applications of Kloosterman sums: cross-correlation functions

- Consider two binary sequences with period $2^m - 1$, $u(t) = \mathrm{Tr}(\alpha^t)$ and $v(t) = u(-t)$.
- The cross-correlation function between $u(t)$ and $v(t)$ is defined by

$$C_t(a) = \sum_{t=0}^{2^m-2} (-1)^{u(t+a)+v(t)} = \sum_{x \in \mathbb{F}_{2^m}^*} (-1)^{\mathrm{Tr}(x^{-1}+ax)} = K(a).$$

- Problem: determine the values and the number of occurrences of each value taken on by $C_t(a)$.

Applications of Kloosterman sums: cross-correlation functions

- Consider two binary sequences with period $2^m - 1$, $u(t) = \mathrm{Tr}(\alpha^t)$ and $v(t) = u(-t)$.
- The cross-correlation function between $u(t)$ and $v(t)$ is defined by

$$C_t(a) = \sum_{t=0}^{2^m-2} (-1)^{u(t+a)+v(t)} = \sum_{x \in \mathbb{F}_{2^m}^*} (-1)^{\mathrm{Tr}(x^{-1}+ax)} = K(a).$$

- Problem: determine the values and the number of occurrences of each value taken on by $C_t(a)$.

Applications of Kloosterman sums: $K(a) = -1$

Open problem: describe elements $a \in \mathbb{F}_{2^m}$ for which $K(a) = -1$.

Theorem (Lachaud, Wolfmann)

The set of $K(a)$, $a \in \mathbb{F}_{2^m}^*$ is the set of all the integers $s \equiv -1 \pmod 4$ in the range

$$[-2^{m/2+1}, 2^{m/2+1}].$$

- Hence there are some $a \in \mathbb{F}_{2^m}$ for which $K(a) = -1$, but their number is still unknown.
- Partial results could narrow down the search field.

Applications of Kloosterman sums: $K(a) = -1$

Open problem: describe elements $a \in \mathbb{F}_{2^m}$ for which $K(a) = -1$.

Theorem (Lachaud, Wolfmann)

The set of $K(a)$, $a \in \mathbb{F}_{2^m}^*$ is the set of all the integers $s \equiv -1 \pmod 4$ in the range

$$[-2^{m/2+1}, 2^{m/2+1}].$$

- Hence there are some $a \in \mathbb{F}_{2^m}$ for which $K(a) = -1$, but their number is still unknown.
- Partial results could narrow down the search field.

Applications of Kloosterman sums: $K(a) = -1$

Open problem: describe elements $a \in \mathbb{F}_{2^m}$ for which $K(a) = -1$.

Theorem (Lachaud, Wolfmann)

The set of $K(a)$, $a \in \mathbb{F}_{2^m}^*$ is the set of all the integers $s \equiv -1 \pmod 4$ in the range

$$[-2^{m/2+1}, 2^{m/2+1}].$$

- Hence there are some $a \in \mathbb{F}_{2^m}$ for which $K(a) = -1$, but their number is still unknown.
- Partial results could narrow down the search field.

Elliptic curve $\mathcal{E}_t$

Let $t \in \mathbb{F}_{2^m}$, $t \notin \{0, 1\}$, and consider the elliptic curve

$$\mathcal{E}_t : \quad y^2 + xy = x^3 + a_2x^2 + (t^8 + t^6),$$

where

$$a_2 = \mathrm{Tr}(t).$$

Later we will show that $\mathcal{E}_t$ arises naturally in the problem of counting coset leaders for the Melas code.

Elliptic curve $\mathcal{E}_t$

Let $t \in \mathbb{F}_{2^m}$, $t \notin \{0,1\}$, and consider the elliptic curve

$$\mathcal{E}_t : \quad y^2 + xy = x^3 + a_2 x^2 + (t^8 + t^6),$$

where

$$a_2 = \mathrm{Tr}(t).$$

Later we will show that $\mathcal{E}_t$ arises naturally in the problem of counting coset leaders for the Melas code.

$3|K(a) \iff a = t^4 + t^3$

Theorem

Let $m \geq 3$ be odd and let $a \in \mathbb{F}_{2^m}^*$. Then $K(a)$ is divisible by 3 if and only if $a = t^4 + t^3$ for some $t \in \mathbb{F}_{2^m}$.

"$\Leftarrow$" (Proved first by Helleseth and Zinoviev, 1999)

- Due to Lachaud and Wolfmann we get

$$\#\mathcal{E}_t = \begin{cases} 2^m + 1 + K(t^4 + t^3) & \text{if } \mathrm{Tr}(t) = 0, \\ 2^m + 1 - K(t^4 + t^3) & \text{if } \mathrm{Tr}(t) = 1. \end{cases}$$

- We find a point on $\mathcal{E}_t$ of order 6, hence $6|\#\mathcal{E}_t$.
- Since $3|(2^m + 1)$, we get $3|K(t^4 + t^3)$.
  (We will later see a more combinatorial proof of $6|\#\mathcal{E}_t$)

$3|K(a) \iff a = t^4 + t^3$

Theorem

Let $m \geq 3$ be odd and let $a \in \mathbb{F}_{2^m}^*$. Then $K(a)$ is divisible by 3 if and only if $a = t^4 + t^3$ for some $t \in \mathbb{F}_{2^m}$.

"$\Leftarrow$" (Proved first by Helleseth and Zinoviev, 1999)

- Due to Lachaud and Wolfmann we get

$$\#\mathcal{E}_t = \begin{cases} 2^m + 1 + K(t^4 + t^3) & \text{if } \mathrm{Tr}(t) = 0, \\ 2^m + 1 - K(t^4 + t^3) & \text{if } \mathrm{Tr}(t) = 1. \end{cases}$$

- We find a point on $\mathcal{E}_t$ of order 6, hence $6|\#\mathcal{E}_t$.
- Since $3|(2^m + 1)$, we get $3|K(t^4 + t^3)$.
  (We will later see a more combinatorial proof of $6|\#\mathcal{E}_t$)

$3|K(a) \iff a = t^4 + t^3$

"$\Rightarrow$"

- Charpin, Helleseth and Zinoviev (2007): $3|K(a) \Leftrightarrow \mathrm{Tr}(a^{1/3}) = 0$
- $\mathrm{Tr}(a^{1/3}) = 0 \Leftrightarrow a = t^4 + t^3$

$\square$

In fact, we can generalize the last equivalence.

Characterization for $\mathrm{Tr}(a^{1/(2^k-1)}) = 0$

Theorem

Let $m > 1$ and let k be such that $\gcd(2^k-1, 2^m-1) = 1$. Then for each $a \in \mathbb{F}_{2^m}$ we have

$$\mathrm{Tr}(a^{1/(2^k-1)}) = 0 \text{ if and only if } a = t^{2^k} + t^{2^k-1}$$

for some $t \in \mathbb{F}_{2^m}$.

(The case $k = 1$ is a well-known fact.)

Binary linear codes

Definition

A binary linear $[n, k, d]$-code C is a k-dimensional linear subspace of $\mathbb{F}_2^n$ such that any two different elements of the code are at Hamming distance at least d.

Definition

H is called a parity check matrix for a linear code C if $x \in C \iff Hx^T = \mathbf{0}$. Then Hx^T is called the syndrome of x.

Definition

A coset leader for a coset D of C is an element of D with the smallest Hamming weight. The weight of a coset is the weight of its coset leader(s).

Melas code $\mathcal{M}_m$

- $\mathbb{F}_{2^m} \simeq \mathbb{F}_2^m$, α a primitive element of $\mathbb{F}_{2^m}$
- The standard parity check matrix of the Melas code $\mathcal{M}_m$ is

$$\mathcal{H}_M = \begin{pmatrix} \alpha & \dots & \alpha^i & \dots & \alpha^{2^m-1} \\ \alpha^{-1} & \dots & \alpha^{-i} & \dots & \alpha^{-(2^m-1)} \end{pmatrix}.$$

- $\mathcal{H}_M$ will be used to produce syndromes. We wish to find the number of coset leaders for a coset of $\mathcal{M}_m$ of weight 3 corresponding to a given syndrome $(a, b)^T \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$.
- The number of coset leaders is the number of different error patterns of weight 3 resulting in the same syndrome and we would like to minimize this quantity.

Melas code $\mathcal{M}_m$

- $\mathbb{F}_{2^m} \simeq \mathbb{F}_2^m$, α a primitive element of $\mathbb{F}_{2^m}$
- The standard parity check matrix of the Melas code $\mathcal{M}_m$ is

$$\mathcal{H}_M = \begin{pmatrix} \alpha & \dots & \alpha^i & \dots & \alpha^{2^m-1} \\ \alpha^{-1} & \dots & \alpha^{-i} & \dots & \alpha^{-(2^m-1)} \end{pmatrix}.$$

- $\mathcal{H}_M$ will be used to produce syndromes. We wish to find the number of coset leaders for a coset of $\mathcal{M}_m$ of weight 3 corresponding to a given syndrome $(a, b)^T \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$.
- The number of coset leaders is the number of different error patterns of weight 3 resulting in the same syndrome and we would like to minimize this quantity.

A system of algebraic equations

- We are led to counting the number of solutions to the following system of equations over $\mathbb{F}_{2^m}^*$:

$$\begin{array}{ccccccc} u & + & v & + & w & = & 1 \\ u^{-1} & + & v^{-1} & + & w^{-1} & = & r \end{array} \qquad (1)$$

  where $r \in \mathbb{F}_{2^m}$ is a fixed constant.
- Consider the general case when $r \notin \{0, 1\}$.

The number of solutions

Theorem

Let $r \in \mathbb{F}_{2^m} \setminus \{0,1\}$. The number of solutions $(u,v,w) \in (\mathbb{F}_{2^m}^*)^3$ of (1) is an integer T such that

- $T \in [2^m + 1 - 2^{m/2+1} - 6\ ,\ 2^m + 1 + 2^{m/2+1} - 6]$
- *6 divides T.*

Conversely, each T satisfying these two conditions occurs as the number of solutions for at least one $r \in \mathbb{F}_{2^m} \setminus \{0,1\}$.

A substitution motivated by Lachaud & Wolfmann

- We eliminate w and homogenize as $u = U/Z$, $v = V/Z$.
- Next we apply the substitution

$$\begin{cases} r = 1 + \dfrac{1}{t}, \\ U = \dfrac{1}{t}x + (t+1)z, \\ V = \dfrac{1}{t^2}(y + sx) + (t^2 + t)z, \\ Z = \dfrac{t+1}{t^2}x + (t+1)z. \end{cases}$$

Note: $r \in \mathbb{F}_{2^m} \setminus \{0,1\}$ implies $t \in \mathbb{F}_{2^m} \setminus \{0,1\}$.

The number of solutions (u, v, w) is $\#\mathcal{E}_t - 6$

We obtain the same curve $\mathcal{E}_t$ as before!

A lot of technical calculations show that exactly 6 points on $\mathcal{E}_t$ do not produce a solution (u, v, w):

- The point at infinity $\mathcal{O} \in \mathcal{E}_t$.
- 3 points on $\mathcal{E}_t$ that correspond to (u, v, w) being a permutation of $(0, 0, 1)$.
- 2 points on $\mathcal{E}_t$ that make the homogenization variable $Z = 0$.

Distinct points on $\mathcal{E}_t$ produce distinct solutions (u, v, w), if any.

The number of solutions (u, v, w) is $\#\mathcal{E}_t - 6$

We obtain the same curve $\mathcal{E}_t$ as before!

A lot of technical calculations show that exactly 6 points on $\mathcal{E}_t$ do not produce a solution (u, v, w):

- The point at infinity $\mathcal{O} \in \mathcal{E}_t$.
- 3 points on $\mathcal{E}_t$ that correspond to (u, v, w) being a permutation of $(0, 0, 1)$.
- 2 points on $\mathcal{E}_t$ that make the homogenization variable $Z = 0$.

Distinct points on $\mathcal{E}_t$ produce distinct solutions (u, v, w), if any.

The proof in one direction is complete:

The assumption $r \neq 1$ forces u, v, w to be distinct in any solution (u, v, w). Thus the number of solutions is divisible by $3! = 6$. This is the combinatorial proof for $6 | \#\mathcal{E}_t$ promised earlier.

By the Hasse Theorem the number of solutions (u, v, w) is in

$$[2^m + 1 - 2^{m/2+1} - 6, 2^m + 1 + 2^{m/2+1} - 6] \cap 6\mathbb{Z}$$

for each $t \in \mathbb{F}_{2^m} \setminus \{0, 1\}$, and hence for each $r \in \mathbb{F}_{2^m} \setminus \{0, 1\}$. $\square$

The proof in one direction is complete:

The assumption $r \neq 1$ forces u, v, w to be distinct in any solution (u, v, w). Thus the number of solutions is divisible by $3! = 6$. This is the combinatorial proof for $6|\#\mathcal{E}_t$ promised earlier.

By the Hasse Theorem the number of solutions (u, v, w) is in

$$[2^m + 1 - 2^{m/2+1} - 6, 2^m + 1 + 2^{m/2+1} - 6] \cap 6\mathbb{Z}$$

for each $t \in \mathbb{F}_{2^m} \setminus \{0, 1\}$, and hence for each $r \in \mathbb{F}_{2^m} \setminus \{0, 1\}$. $\square$

The coset leaders and the symmetry

Corollary

Let $m \geq 3$ be an odd integer. Let $a, b \in \mathbb{F}_{2^m}^*$, $a \neq b$. Suppose that the syndrome $(a, b)^T$ corresponds to a coset D of weight 3 of $\mathcal{M}_m$. Then the number of coset leaders of D is an integer L such that

$$6L \in [2^m + 1 - 2^{m/2+1} - 6, 2^m + 1 + 2^{m/2+1} - 6].$$

Conversely, each such L occurs as the number of coset leaders for at least one such coset D.

Theorem

Let $N(k)$ denote the number of those $r \in \mathbb{F}_{2^m} \setminus \{0, 1\}$ for which the number of solutions to (1) is equal to k. Then for each $l \in \mathbb{N}$ we have $N(2^m - 5 + l) = N(2^m - 5 - l)$. That is, the values $N(k)$ are symmetric about $k = 2^m - 5$.

The coset leaders and the symmetry

Corollary

Let $m \geq 3$ be an odd integer. Let $a, b \in \mathbb{F}_{2^m}^*$, $a \neq b$. Suppose that the syndrome $(a, b)^T$ corresponds to a coset D of weight 3 of $\mathcal{M}_m$. Then the number of coset leaders of D is an integer L such that

$$6L \in [2^m + 1 - 2^{m/2+1} - 6, 2^m + 1 + 2^{m/2+1} - 6].$$

Conversely, each such L occurs as the number of coset leaders for at least one such coset D.

Theorem

Let $N(k)$ denote the number of those $r \in \mathbb{F}_{2^m} \setminus \{0, 1\}$ for which the number of solutions to (1) is equal to k. Then for each $l \in \mathbb{N}$ we have $N(2^m - 5 + l) = N(2^m - 5 - l)$. That is, the values $N(k)$ are symmetric about $k = 2^m - 5$.

Caps with many free pairs of points

- A cap in $\mathrm{PG}(n, 2)$ is a set C of points such that no three of them are collinear.
- Points of C are columns of the parity check matrix H_C for a code of minimum distance 4 (or more).
- We say that $\{s, t\} \subset C$ is a free pair of points if $\{s, t\}$ is not contained in any coplanar quadruple of C.
- Clearly, all pairs of points of C are free if and only if H_C defines a code of minimum distance 5 (or more).

Caps with many free pairs of points

- A cap in $\mathrm{PG}(n, 2)$ is a set C of points such that no three of them are collinear.
- Points of C are columns of the parity check matrix H_C for a code of minimum distance 4 (or more).
- We say that $\{s, t\} \subset C$ is a free pair of points if $\{s, t\}$ is not contained in any coplanar quadruple of C.
- Clearly, all pairs of points of C are free if and only if H_C defines a code of minimum distance 5 (or more).

Motivation

Application: statistical experiment design - caps with many free pairs of points are known as clear two-factor interactions.

The goal: Given the size (number of points) of the cap and its projective dimension, maximize the number of free pairs of points in the cap.

Construction based on linear codes of distance 5

- Start with the parity check matrix H^* of a binary linear code of distance 5 and carefully add columns to it.
- If z is a newly added column and if a, b, c are three columns of H^* such that $a + b + c = z$, then the free pairs $\{a, b\}$, $\{a, c\}$ and $\{b, c\}$ are destroyed.
- It is therefore desirable to add to H^* syndromes z that correspond to cosets of weight 3 such that the number of coset leaders is minimized.

Highly nonlinear functions

- Let $f : \mathbb{F}_{p^m} \mapsto \mathbb{F}_{p^m}$ and let $N(a,b)$ be the number of solutions $x \in \mathbb{F}_{p^m}$ of $f(x+a) - f(x) = b$, $a, b \in \mathbb{F}_{p^m}$. Consider

$$\nabla_f = \max\{N(a,b) : a \in \mathbb{F}^*_{p^m}, b \in \mathbb{F}_{p^m}\}.$$

- The smaller the value of ∇_f, the further f is from being linear.
- $\nabla_f = 1 \quad \ldots \quad f : \mathbb{F}_{p^m} \mapsto \mathbb{F}_{p^m}$ is a perfect nonlinear function
- $\nabla_f = 2 \quad \ldots \quad f : \mathbb{F}_{2^m} \mapsto \mathbb{F}_{2^m}$ is almost perfect nonlinear
- Notice that the solutions to $f(x+a) - f(x) = b$ in $\mathbb{F}_{2^m}$ occur in pairs $\{x_0, x_0 + a\}$, hence the *almost* perfect nonlinear.

Highly nonlinear functions

- Let $f : \mathbb{F}_{p^m} \mapsto \mathbb{F}_{p^m}$ and let $N(a,b)$ be the number of solutions $x \in \mathbb{F}_{p^m}$ of $f(x+a) - f(x) = b$, $a, b \in \mathbb{F}_{p^m}$. Consider

$$\nabla_f = \max\{N(a,b) : a \in \mathbb{F}^*_{p^m}, b \in \mathbb{F}_{p^m}\}.$$

- The smaller the value of ∇_f, the further f is from being linear.
- $\nabla_f = 1 \quad \ldots \quad f : \mathbb{F}_{p^m} \mapsto \mathbb{F}_{p^m}$ is a perfect nonlinear function
- $\nabla_f = 2 \quad \ldots \quad f : \mathbb{F}_{2^m} \mapsto \mathbb{F}_{2^m}$ is almost perfect nonlinear
- Notice that the solutions to $f(x+a) - f(x) = b$ in $\mathbb{F}_{2^m}$ occur in pairs $\{x_0, x_0 + a\}$, hence the *almost* perfect nonlinear.

APN functions on $\mathbb{F}_{2^m}$ and codes of distance 5

Theorem

(Carlet, Charpin and Zinoviev (1998)) Let $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, $f(0) = 0$. *Let* C_f *be the binary code defined be the parity check matrix*

$$\mathcal{H}_f = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{2^m-1} \\ f(1) & f(\alpha) & f(\alpha^2) & \cdots & f(\alpha^{2^m-1}) \end{pmatrix}.$$

Then f *is almost perfect nonlinear (APN) if and only if* $d = 5$.

Almost bent functions

Definition (Fourier Transform)

The Fourier transform of f $\mu_f : \mathbb{F}_2^m \times \mathbb{F}_2^m \to \mathbb{Z}$ *is defined as follows:*

$$\mu_f(a,b) = \sum_{x \in \mathbb{F}_2^m} (-1)^{\langle a,x \rangle} (-1)^{\langle b,f(x) \rangle},$$

where $a, b \in \mathbb{F}_{2^m}$ *and* $\langle \cdot, \cdot \rangle$ *denotes the standard inner product.*

Definition (Almost Bent Function)

A mapping f from $\mathbb{F}_2^m$ *to itself is called almost bent (AB) if* $\mu_f(a,b) \in \{0, \pm 2^{(m+1)/2}\}$ *for all* $(a,b) \neq (0,0)$.

Note: AB functions exist only for m odd.

Number of solutions for AB functions

Theorem

(van Dam and Fon-Der-Flaass, 2003) A function $f : \mathbb{F}_2^m \to \mathbb{F}_2^m$ is AB if and only if the system

$$\begin{cases} u + v + w = a \\ f(u) + f(v) + f(w) = b \end{cases}$$

has $q-2$ or $3q-2$ solutions (u, v, w) for every (a, b), where $q = 2^m$. If so, then the system has $3q-2$ solutions if $b = f(a)$ and $q-2$ solutions otherwise.

$$\mathcal{AB} \subset \mathcal{APN}$$

Construction based on APN functions: Summary

- Recall: We start with the parity check matrix H^* of a binary linear code of distance 5. Let's restrict to codes defined by APN functions.
- We add to H^* syndromes that correspond to cosets of weight 3 for which the number of coset leaders is small.
- In (Lisonek, 2006) this was worked out for the Gold function $f(x) = x^3$ on $\mathbb{F}_{2^m}$ (BCH codes). When m is odd, Gold functions are AB and van Dam & Fon-Der-Flaass theorem applies: the number of solutions is always $q - 2$.

Construction based on APN functions: Summary

- Recall: We start with the parity check matrix H^* of a binary linear code of distance 5. Let's restrict to codes defined by APN functions.
- We add to H^* syndromes that correspond to cosets of weight 3 for which the number of coset leaders is small.
- In (Lisonek, 2006) this was worked out for the Gold function $f(x) = x^3$ on $\mathbb{F}_{2^m}$ (BCH codes). When m is odd, Gold functions are AB and van Dam & Fon-Der-Flaass theorem applies: the number of solutions is always $q - 2$.

Comparison of Gold and Inverse functions

- On the other hand, $f(x) = x^{-1}$ is APN for m odd, but not AB. Therefore, the number of solutions can be as low as roughly $q - 2\sqrt{q}$, thus yielding a further improvement.
- Moreover, the distribution of the number of solutions for $f(x) = x^{-1}$ is symmetric about $q - 5$. Consequently, roughly one half of the choices for syndromes yield better results than what can be achieved when using $f(x) = x^3$.

Comparison of Gold and Inverse functions

- On the other hand, $f(x) = x^{-1}$ is APN for m odd, but not AB. Therefore, the number of solutions can be as low as roughly $q - 2\sqrt{q}$, thus yielding a further improvement.
- Moreover, the distribution of the number of solutions for $f(x) = x^{-1}$ is symmetric about $q - 5$. Consequently, roughly one half of the choices for syndromes yield better results than what can be achieved when using $f(x) = x^3$.

Ternary Kloosterman sums

Recall that Kloosterman sums over $\mathbb{F}_{3^m}$ are defined as follows:

$$K(a) := \sum_{x \in \mathbb{F}_{3^m}^*} \left(-\frac{1}{2} + \frac{\sqrt{3}}{2} i \right)^{\mathrm{Tr}(x^{-1} + ax)} .$$

Moisio's result

Theorem (Moisio, 2007)

Let $c \in \mathbb{F}_{3^m}^*$ and let Φ be an elliptic curve over $\mathbb{F}_{3^m}$ defined by

$$\Phi : \quad y^2 = x^3 + x^2 - c.$$

Then $\#\Phi = 3^m + 1 + K(c)$.

We use this connection between ternary Kloosterman sums and ternary elliptic curves to classify and count those $a \in \mathbb{F}_{3^m}$ for which $K(a) \equiv 0, 2 \pmod 4$.

Moisio's result

Theorem (Moisio, 2007)

Let $c \in \mathbb{F}_{3^m}^*$ *and let* Φ *be an elliptic curve over* $\mathbb{F}_{3^m}$ *defined by*

$$\Phi : \quad y^2 = x^3 + x^2 - c.$$

Then $\#\Phi = 3^m + 1 + K(c)$.

We use this connection between ternary Kloosterman sums and ternary elliptic curves to classify and count those $a \in \mathbb{F}_{3^m}$ for which $K(a) \equiv 0, 2 \pmod 4$.

Properties of ternary Kloosterman sums

Lemma

$K(a)$ is an integer for all $a \in \mathbb{F}_{3^m}$.

Lemma

Let $a \in \mathbb{F}_{3^m}$. Let $N(a)$ denote the number of solutions $x \in \mathbb{F}_{3^m}^*$ to the equation $\mathrm{Tr}(x^{-1} + ax) = 1$. Then $K(a) \equiv N(a) \pmod 2$.

Lemma

Let $a \in \mathbb{F}_{3^m}$. Then $K(a) \equiv 2 \pmod 3$.

Properties of ternary Kloosterman sums

Lemma

$K(a)$ is an integer for all $a \in \mathbb{F}_{3^m}$.

Lemma

Let $a \in \mathbb{F}_{3^m}$. Let $N(a)$ denote the number of solutions $x \in \mathbb{F}_{3^m}^*$ to the equation $\mathrm{Tr}(x^{-1} + ax) = 1$. Then $K(a) \equiv N(a) \pmod 2$.

Lemma

Let $a \in \mathbb{F}_{3^m}$. Then $K(a) \equiv 2 \pmod 3$.

Properties of ternary Kloosterman sums

Lemma

$K(a)$ is an integer for all $a \in \mathbb{F}_{3^m}$.

Lemma

Let $a \in \mathbb{F}_{3^m}$. Let $N(a)$ denote the number of solutions $x \in \mathbb{F}_{3^m}^*$ to the equation $\mathrm{Tr}(x^{-1} + ax) = 1$. Then $K(a) \equiv N(a) \pmod 2$.

Lemma

Let $a \in \mathbb{F}_{3^m}$. Then $K(a) \equiv 2 \pmod 3$.

Properties of ternary Kloosterman sums (continued)

Theorem

$K(a)$ is odd if and only if $a = 0$ or a is a square and $\mathrm{Tr}(\sqrt{a}) \neq 0$.

Corollary

$K(a)$ is odd for $3^{m-1} + 1$ elements $a \in \mathbb{F}_{3^m}$.

System of equations

- Consider the following system of equations over $\mathbb{F}_{3^m}^*$:

$$\begin{array}{ccccccc} u & + & v & + & w & = & 1, \\ u^{-1} & + & v^{-1} & + & w^{-1} & = & 1/t, \end{array} \qquad (2)$$

  where $t \in \mathbb{F}_{3^m} \setminus \{0, 1\}$ is a fixed constant.
- Let $S(1/t)$ denote the total number of solutions to (2).

Grouping solutions

- We can pair up the solutions: (u, v, w) and $(\frac{t}{u}, \frac{t}{v}, \frac{t}{w})$.
- We wish to see how many distinct ordered solutions there are in the set composed of all permutations of (u, v, w) and all permutations of $(\frac{t}{u}, \frac{t}{v}, \frac{t}{w})$.
- In most cases there will be 12 triples in total except when $|\{u, v, w\}| < 3$ or $(\frac{t}{u}, \frac{t}{v}, \frac{t}{w})$ is a permutation of (u, v, w).

Grouping solutions

- We can pair up the solutions: (u, v, w) and $(\frac{t}{u}, \frac{t}{v}, \frac{t}{w})$.
- We wish to see how many distinct ordered solutions there are in the set composed of all permutations of (u, v, w) and all permutations of $(\frac{t}{u}, \frac{t}{v}, \frac{t}{w})$.
- In most cases there will be 12 triples in total except when $|\{u, v, w\}| < 3$ or $(\frac{t}{u}, \frac{t}{v}, \frac{t}{w})$ is a permutation of (u, v, w).

Number of solutions modulo 12

Theorem

Let $t \in \mathbb{F}_{3^m} \setminus \{0, 1\}$.

$$S(1/t) \equiv \begin{cases} 6 \pmod{12} & \textit{if } t \textit{ or } 1\text{-}t \textit{ is a square}, \\ 0 \pmod{12} & \textit{otherwise}. \end{cases}$$

Elliptic curve

Let $\bar{\mathcal{E}}_t$ denote the following elliptic curve over $\mathbb{F}_{3^m}$:

$$\bar{\mathcal{E}}_t : \quad y^2 = x^3 + x^2 - (t^6 - t^9).$$

Theorem

Let $t \in \mathbb{F}_{3^m} \setminus \{0,1\}$. Then

$$S(1/t) = \#\bar{\mathcal{E}}_t - 6,$$

where $\#\bar{\mathcal{E}}_t$ denotes the number of points on $\bar{\mathcal{E}}_t$ over $\mathbb{F}_{3^m}$.

Idea for the proof

- As in the binary case we eliminate w, homogenize the resulting equation and use a substitution to obtain an elliptic curve in Weierstrass form, denote it by $\bar{\mathcal{E}}_r$.
- There are 6 points on $\bar{\mathcal{E}}_r$ that do not correspond to a solution of (2).
- We then apply another substitution to obtain $\bar{\mathcal{E}}_t$. Since the two curves are isomorphic, we have $\#\bar{\mathcal{E}}_r = \#\bar{\mathcal{E}}_t$, so $S(1/t) = \#\bar{\mathcal{E}}_t - 6$.

Idea for the proof

- As in the binary case we eliminate w, homogenize the resulting equation and use a substitution to obtain an elliptic curve in Weierstrass form, denote it by $\bar{\mathcal{E}}_r$.
- There are 6 points on $\bar{\mathcal{E}}_r$ that do not correspond to a solution of (2).
- We then apply another substitution to obtain $\bar{\mathcal{E}}_t$. Since the two curves are isomorphic, we have $\#\bar{\mathcal{E}}_r = \#\bar{\mathcal{E}}_t$, so $S(1/t) = \#\bar{\mathcal{E}}_t - 6$.

Partitioning of $\mathbb{F}_{3^m}$

Theorem

Let $m \geq 3$ and let

$$A_1 = \{a \in \mathbb{F}_{3^m} | a = 0 \text{ or } a \text{ is a square and } \mathrm{Tr}(\sqrt{a}) \neq 0\},$$

$$A_2 = \{a \in \mathbb{F}_{3^m} | a = t^2 - t^3 \text{ for some } t \in \mathbb{F}_{3^m} \setminus \{0,1\}, \\ t \text{ or } 1 - t \text{ is a square}\},$$

$$A_3 = \{a \in \mathbb{F}_{3^m} | a = t^2 - t^3 \text{ for some } t \in \mathbb{F}_{3^m} \setminus \{0,1\}, \\ \text{both } t \text{ and } 1 - t \text{ are non-squares}\}.$$

Then the sets A_1, A_2, A_3 partition $\mathbb{F}_{3^m}$.

Kloosterman sums modulo 4

Corollary

Let $m \geq 3$ and $a \in \mathbb{F}_{3^m}$. Then exactly one of the following cases occurs:

- $a \in A_1$ *and* $K(a) \equiv 1 \pmod 2$,
- $a \in A_2$ *and* $K(a) \equiv 2m + 2 \pmod 4$,
- $a \in A_3$ *and* $K(a) \equiv 2m \pmod 4$.

Kloosterman sums modulo 4 (continued)

Theorem

Parity of m	$K(a)$	*Number of* $a \in \mathbb{F}_{3^m}^*$
m *is even*	$0 \pmod 4$	$q/4 - 1/4$
	$2 \pmod 4$	$5q/12 - 3/4$
m *is odd*	$0 \pmod 4$	$5q/12 - 5/4$
	$2 \pmod 4$	$q/4 + 1/4$

New ternary quasi-perfect codes

- Danev and Dodunekov (2008) constructed a new family of ternary quasi-perfect codes with minimum distance 5 and covering radius 3.
- A major step in their proof is showing that the system (2) is solvable over $\mathbb{F}_{3^m}^*$ for any t. This is done by explicitly finding a solution.
- We offer an alternative proof of the solvability of (2) over $\mathbb{F}_{3^m}$.